CBR-970/971

Wireless-N Broadband Router
Wireless-N 3.5G Broadband Router

User Manual

Version 1.00
(Feb, 2011)

Table of Contents

TABLE OF CONTENTS 2

PREFACE 5

CHAPTER 1 INTRODUCTION 6

1.1 About CBR-970/971 6
1.2 Main Features 6
1.3 System Requirements 6
1.4 Getting to Know CBR-970/971 7
1.4.1 Hardware Specifications 9

CHAPTER 2 SYSTEM AND NETWORK SETUP 10

2.1 Build Network Connection (Router mode) 10
2.2 Build Network Connection (AP mode) 11
2.3 Build Network Connection (WiFi-AP mode) 12
2.4 Connecting to CBR-970/971 by using Web Browser 13
2.4.1 Windows 95/98/ME 13
2.4.2 Windows 2000 15
2.4.3 Windows XP 17
2.4.4 Windows Vista / Windows 7 19
2.4.5 Router IP Address Lookup 21
2.4.6 Connect the Wireless Router's management Interface by Web Browser 22

CHAPTER 3 OPERATION MODES AND ONE BUTTON SETUP 24

CHAPTER 4 ROUTER MODE ADVANCED CONFIGURATION 26

4.1 IP Configuration 26
4.1.1 WAN Interface Setup 26
4.1.1.1 WAN Interface – Ethernet Port 27
4.1.1.1.1 WAN Access Type – Static IP 28
4.1.1.1.2 WAN Access -- Dynamic IP 31
4.1.1.1.3 WAN Access Type -- PPPoE 34
4.1.1.1.4 WAN Access Type -- PPTP 37
4.1.1.1.5 WAN Access Type – L2TP 40
4.1.1.2 WAN Interface – 3.5G (HSDPA/UMTS) (CBR-971 only) 43
4.1.1.3 WAN Access Type – WiMAX (CBR-971 only) 46
4.1.1.4 WAN Access Type – Wireless 48
4.1.2 LAN Interface Setup 49
4.1.3 Dynamic DNS Setting 50
4.2 Wireless Setup 52
4.2.1 Wireless Basic Settings 52
4.2.1.1 Multiple APs 55
4.2.1.2 Enable Universal Repeater Mode (Acting as AP Client simultaneously) 56
4.2.2 Wireless Advanced Settings 58
4.2.3 Wireless Security Setup 60

4.2.4 Wireless Access Control 63
4.2.5 WDS Settings 66
4.2.6 WPS 72
4.3 NAT 80
4.3.1 Virtual Server 80
4.3.2 DMZ 81
4.4 Firewall 82
4.4.1 Port Filtering 83
4.4.2 IP Filtering 84
4.4.3 MAC Filtering 85
4.4.4 URL Filtering 86
4.5 System Management 87
4.5.1 Change Password 87
4.5.2 Firmware Upgrade 88
4.5.3 Profile Save 89
4.5.4 Time Zone Setting 93
4.5.5 UPnP Setting 94
4.6 VPN Passthrough Settings 95
4.7 Log & Status 96
4.7.1 Network Config 96
4.7.2 Event Log 97
4.8 Logout 98

CHAPTER 5 AP MODE ADVANCED CONFIGURATION 99

5.1 IP Config 99
5.1.1 LAN Setup 99
5.1.2 LAN Interface Setup 99
5.2 Wireless Setup 101
5.2.1 Wireless Basic Settings 102
5.2.1.1 Multiple APs 104
5.2.2 Wireless Advanced Settings 105
5.2.3 Wireless Security Setup 107
5.2.4 Wireless Access Control 109
5.2.5 WDS Settings 111
5.2.6 WPS 117
5.3 System Management 118
5.3.1 Change Password 118
5.3.2 Firmware Upgrade 118
5.3.1 Profile Save 120
5.3.2 Time Zone Setting 125
5.3.3 UPnP Setting 126
5.4 Log & Status 127
5.4.1 Network Config 127
5.4.2 Event Log 128
5.5 Logout 130

CHAPTER 6 ADVANCED CONFIGURATION FOR WI-FI AP MODE 131

6.1 IP Config 131
6.1.1 IP Config -- LAN 131
6.1.2 LAN Interface Setup 131
6.2 Wireless Setup 133
6.2.1 Wireless Basic Setting 133
6.2.2 Wireless Advanced Settings 136
6.2.3 Wireless Site Survey 138
6.2.4 Wireless Security Setup 138
6.2.5 Wireless Access Control 141
6.2.6 WPS Setting 143
6.3 System Management 144
6.3.1 Change Password 144
6.3.2 Firmware Upgrade 145
6.3.1 Profile Save 146
6.3.2 Time Zone Setting 150
6.3.3 UPnP Setting 152
6.4 Log & Status 152
6.4.1 Network Config 153
6.4.2 Event Log 153
6.5 Logout 154

CHAPTER 7 DDNS ACCOUNT SETUP 155

CHAPTER 8 Q & A 161

8.1 Installation 161
8.2 LED 161
8.3 IP Address 162
8.4 OS Setting 162
8.5 11n Broadband Router Setup 163
8.6 Wireless LAN 165
8.7 Support 167
8.8 Others 168

Preface

About This Manual

Thank you for purchasing the CBR-970/971 Wireless-N Pico 3.5G Broadband Router. This User's Manual is intended for audience with basic networking knowledge and is the primary reference for configuring and maintaining the device. This manual includes description of the management interface and detailed instruction in its use.

Conventions Used

- Notes, warnings or cautions are in bold with shaded background.
- In this manual, the CBR-970/971 Wireless-N (3.5G) Broadband Router is referred to as "the wireless router".

Chapter 1 Introduction

1.1 About CBR-970/971

CBR-970 is a small wireless broadband router; it provides Ethernet link interfaces and connects to Internet via broadband DSL/Cable modems (and USB interface 3.5G dongles for CBR-971). Additionally it automatically detects user environment's WAN settings to achieve intelligent "Plug & Play", thus making internet experience easier and more enjoyable.

While sharing internet connection with multiple computers, CBR-970 uses security mechanisms such as firewall and QoS to ensure the security level and connection quality of the networking environment. It is a networking solution designed specifically for household and personal applications, emphasizing high security, reliability and ease of use.

CBR-970's unique power saving feature, including Green AP function, helps to reduce up to 80% power consumption when there is no network traffic detected.

1.2 Main Features

The following lists are the main features of the Wireless Router

- Easy management via simple Web GUI.
- Uses QoS to ensure high quality internet connection.
- Advanced firewall security with DoS prevention
- Supports VPN pass-through for high security level VPN connections.
- Automatic WAN type detection.
- Complies with IEEE 802.11n and backward compatible with IEEE 802.11b/g
- Supports Multiple-AP application (up to 4 SSIDs)
- Supports one touch encryption method (WPS) to simplify the secure establishment of a wireless network
- Advanced wireless security, supports 64/128 bit WEP / WPA / WPA2 / WPA2 Mixed
- Supports 3.5G Internet connection (CBR-971 only)

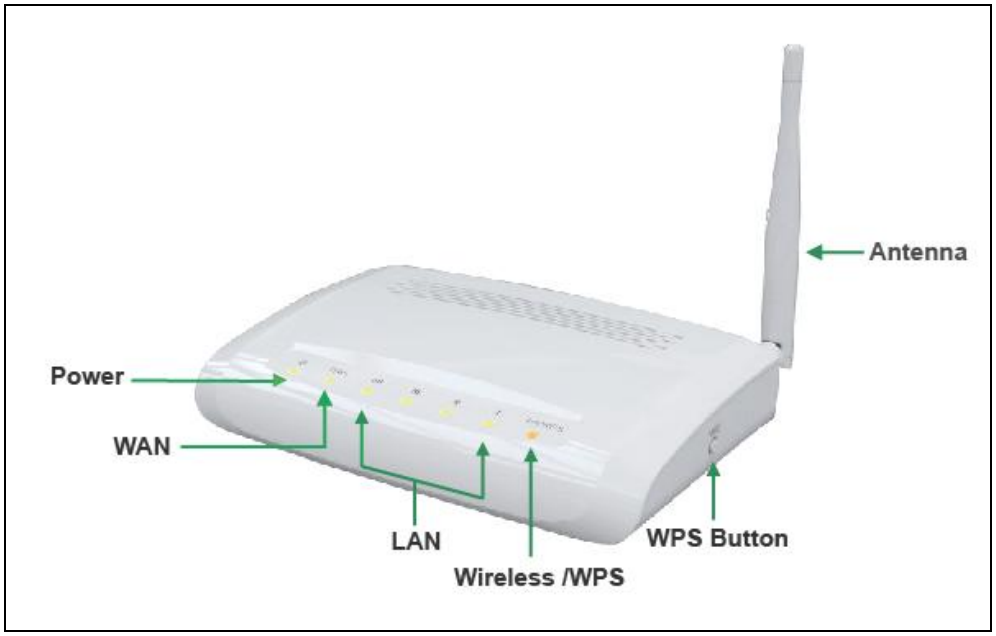
1.3 System Requirements

- Internet connections provided via xDSL/cable modem with a RJ-45 Ethernet port or 3.5G/WiMAX mobile Internet connections.

- Computer or network devices with wired or wireless network interface card.
- Web browser (*Microsoft Internet Explorer 4.0 or above, Netscape Navigator 4.7 or above, Opera web browser, or Safari web browser).*
- An available AC power socket.

1.4 Getting to Know CBR-970/971

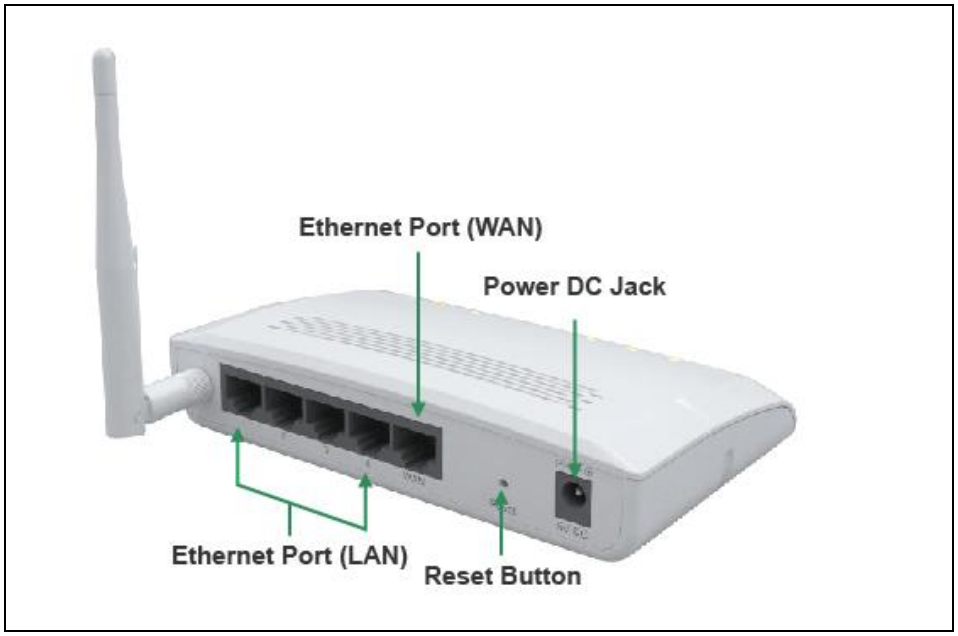
The front view of CBR-970/971



LED	Function	Color	Status	Description
Power x 1	System status	**Green**	On	System is ready to work
			Blinking 120ms	1. Power is being applied and system boot in progress 2. Reset or firmware upgrade in progress
Wireless / WPS x 1	Wireless activity & WPS status	**Green**	On	Wireless is connected
			Blinking 30ms	Wireless Tx/Rx activity
		Reddish Orange	Blinking 120ms	WPS function in progress

WAN x 1	WAN port activity	**Green**	On	100Mbps Ethernet is connected
			Blinking 30ms	100Mbps Ethernet Tx/Rx activity
		Green	On	10Mbps Ethernet is connected
			Blinking 120ms	10Mbps Ethernet Tx/Rx activity
LAN x 4	LAN port activity	**Green**	On	100Mbps Ethernet is connected
			Blinking 30ms	100Mbps Ethernet Tx/Rx activity
		Green	On	10Mbps Ethernet is connected
			Blinking 120ms	10Mbps Ethernet Tx/Rx activity

The back view of CBR-970/971



1.4.1 Hardware Specifications

The following table shows the technical specifications of the wireless router.

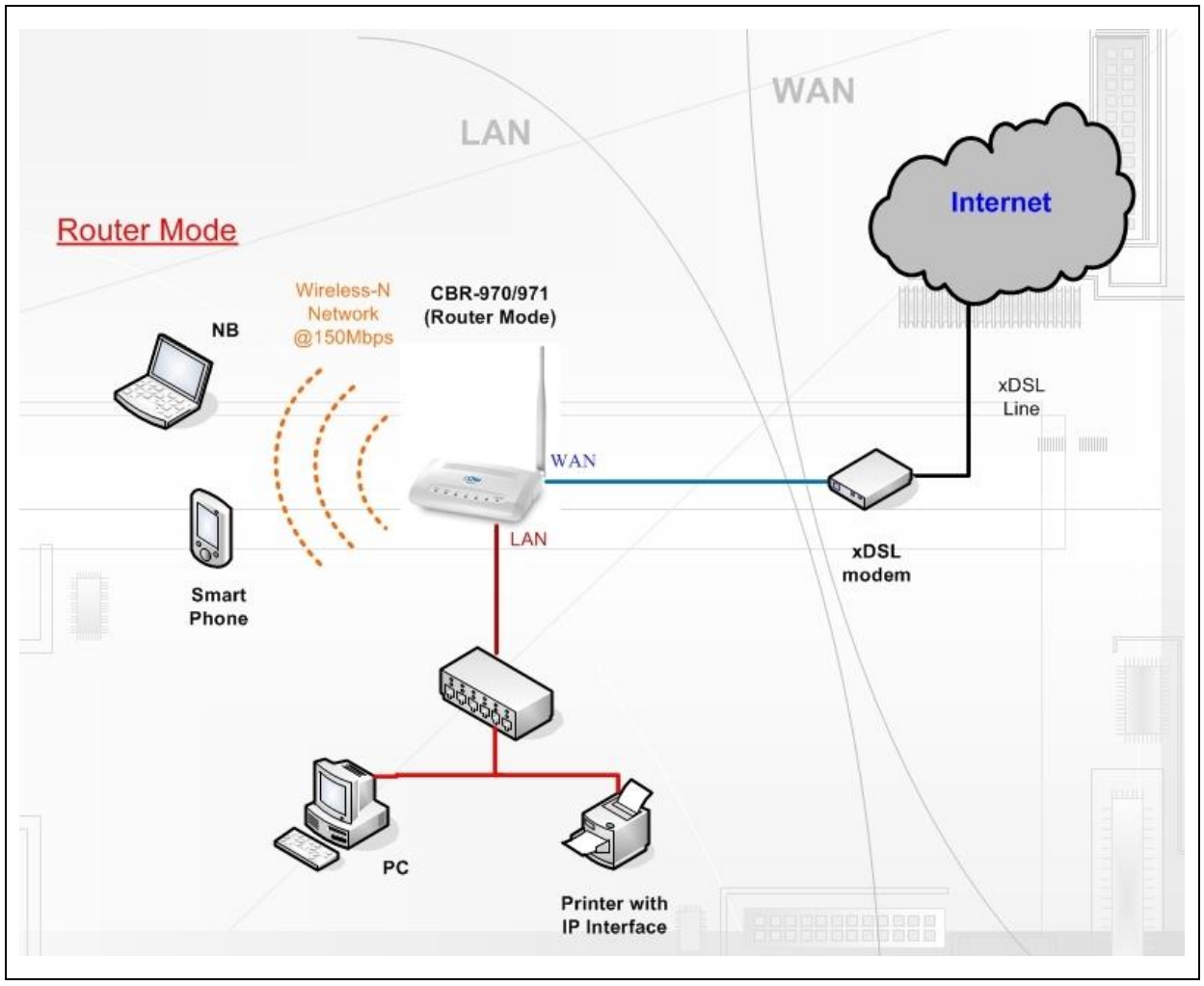
Item	Specifications
Communication Interface	
WAN/LAN Port	1 x 10/100Mbps RJ-45, with auto MDI/MDIX
LAN Port	4 x 10/100Mbps RJ-45, with auto MDI/MDIX
USB Port (CBR-971 only)	USB 2.0 port x 1
Wireless	IEEE 802.11b/g/n
Others	
Operation Requirement	Operating Temp: 0° to 40°C (32° to 10°F) Storage Temp: -20° to 70°C (-4° to 158°F) Operating Humidity: 10% to 85% Non-Condensing Storage Humidity: 5% to 90% Non-Condensing
Antenna	External antenna x 1
Peak Gain of the antenna	3dBi@ 2.45GHz
Transmitted Power	IEEE 802.11b: 19dBm +/- 2.0dBm (typical) IEEE 802.11g: 16dBm +/- 2.0dBm (typical) IEEE 802.11n: 14dBm +/- 1.5dBm (typical)
Receive Sensitivity	IEEE 802.11b: -83dBm +/- 2.0dBm IEEE 802.11g: -70dBm +/- 2.0dBm IEEE 802.11n (20MHz): -74dBm +/- 2.0dBm IEEE 802.11n (20MHz): -74dBm +/- 2.0dBm
Dimension (L x W x H)	145.1 x 89.9 x 31.7 mm (without antenna)
Button	Reboot / Reset button WPS button
Power Supply	Power Adapter DC5V / 0.6A (1.0A for CBR-971)
Certification	CE / FCC / RoHS

Chapter 2 System and Network Setup

The CBR-970/971 is an easy to setup and wireless device for various application and environment. It can be used in conference room, hotel, even in transportation.

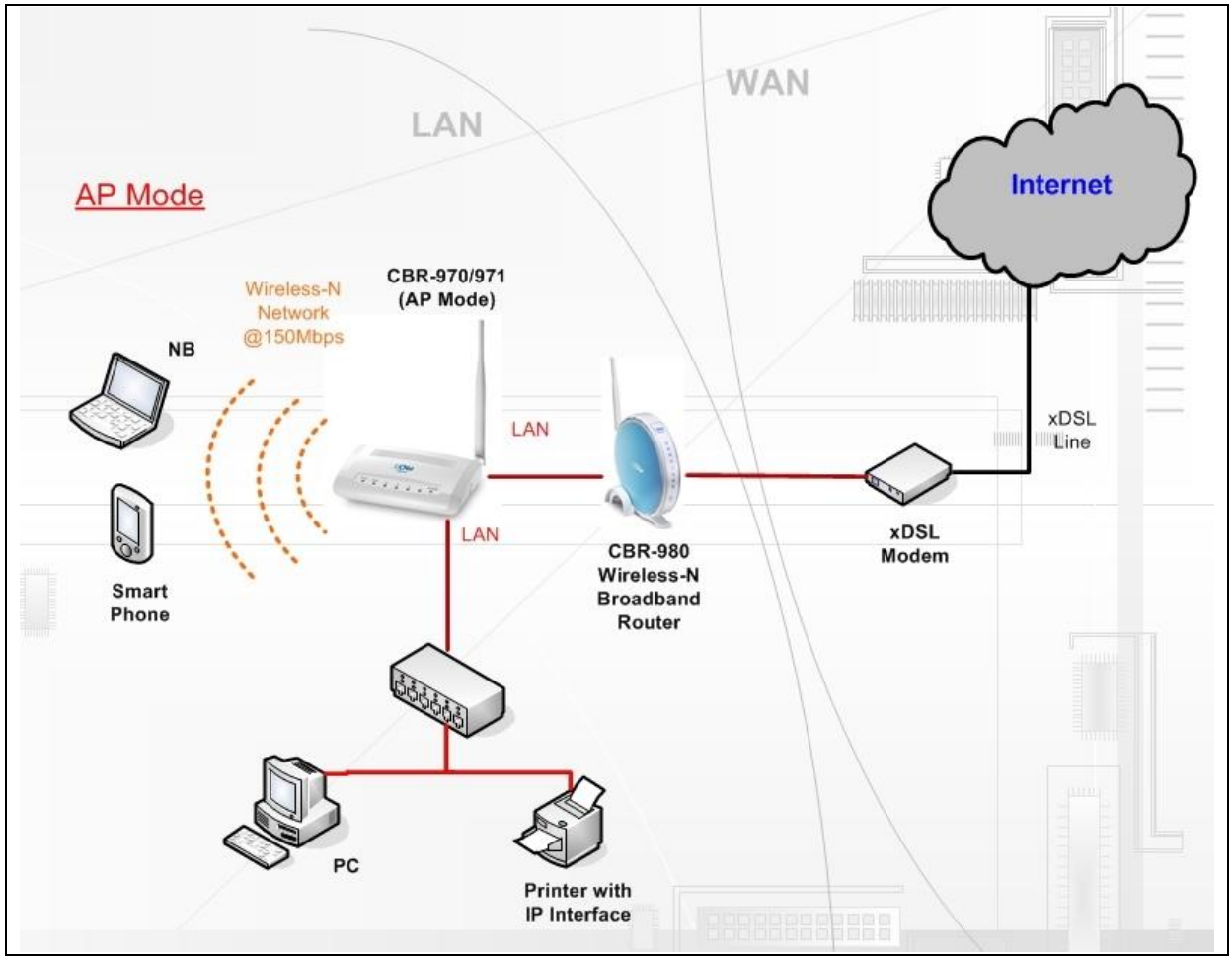
2.1 Build Network Connection (Router mode)

Administrator can manage the settings for WAN, LAN, Wireless Network, NTP, password, User Accounts, Firewall, etc.



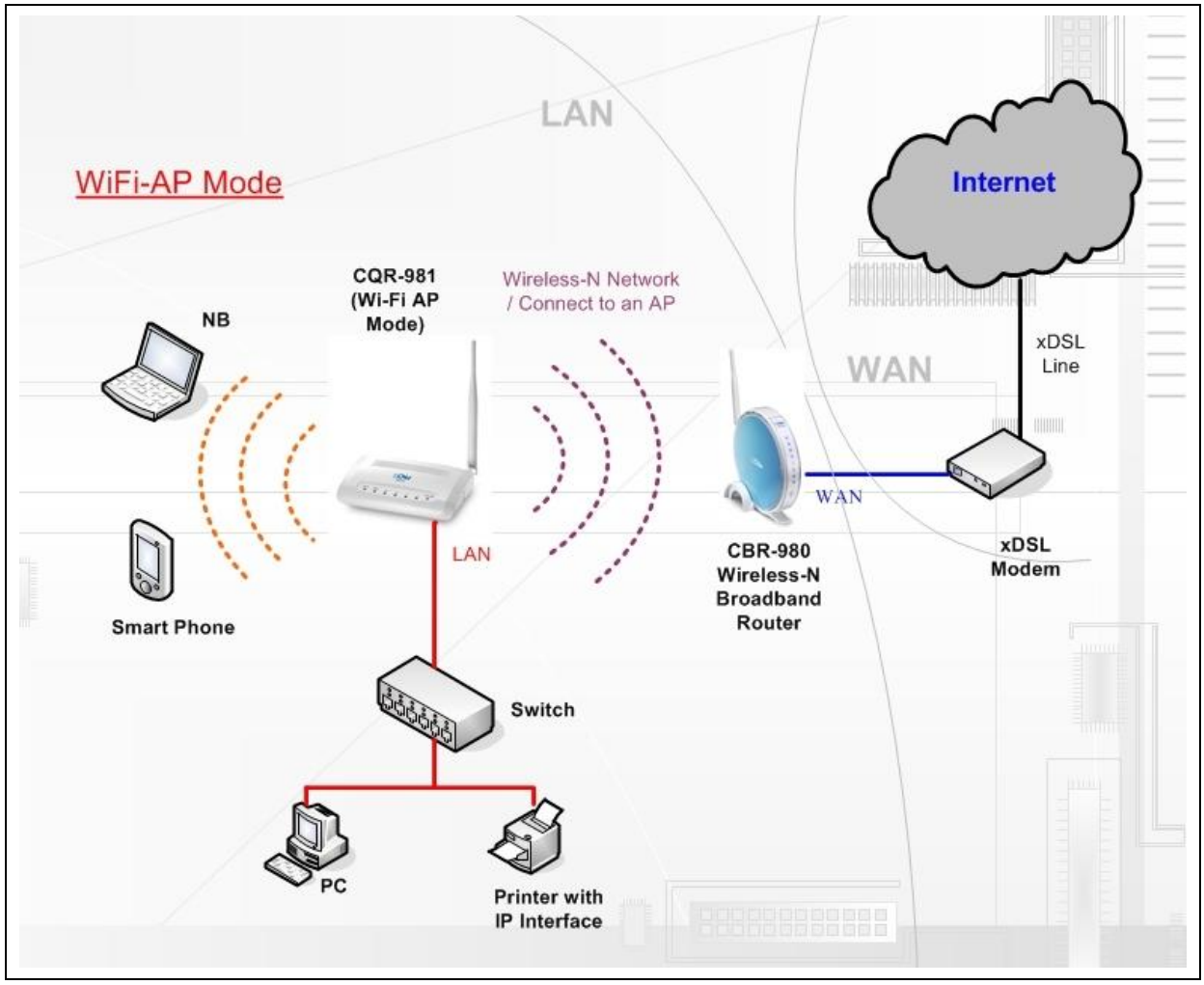
2.2 Build Network Connection (AP mode)

Administrator can manage the settings for WAN, LAN, Wireless Network, NTP, password, User Accounts, Firewall, etc.



2.3 Build Network Connection (WiFi-AP mode)

Administrator can manage the settings for WAN, LAN, Wireless Network, NTP, password, User Accounts, Firewall, etc.



2.4 Connecting to CBR-970/971 by using Web Browser

After the network connection is built, the next step what you should do is setup the router with proper network parameters, so it can work properly in your network environment.

Before you connect to the wireless router and start configuration procedures, your computer must be able to get an IP address from the wireless router automatically (use dynamic IP address). If it's set to use static IP address, or you're unsure, please follow the below instructions to configure your computer with dynamic IP address:

If the operating system of your computer is….

Windows 95/98/ME - please go to section 2.4.1

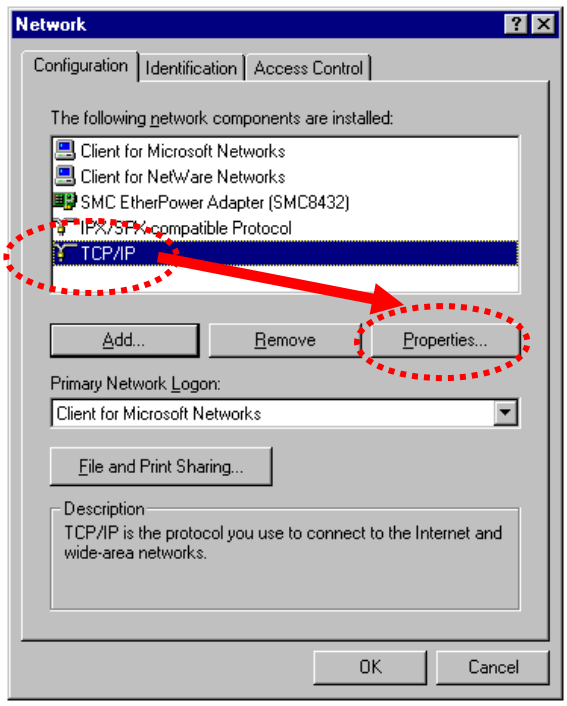
Windows 2000 - please go to section 2.4.2

Windows XP - please go to section 2.4.3

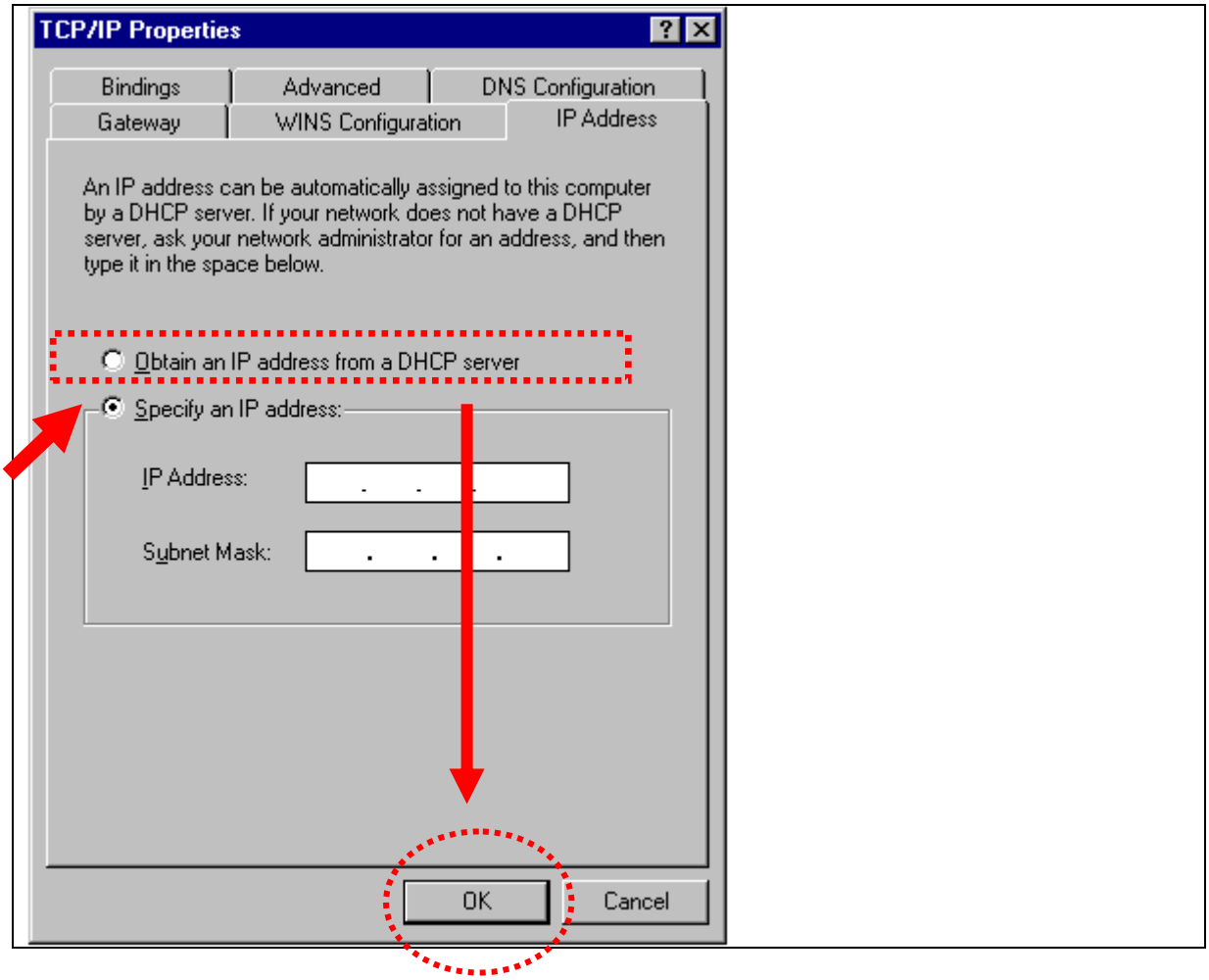
Windows Vista/7 - please go to section 2.4.4

2.4.1 Windows 95/98/ME

1. Click '**Start**' button (it should be located at lower-left corner of your computer), then click control panel. Double-click ***Network*** icon, and ***Network*** window will appear. Select '**TCP/IP**', then click 'Properties'.

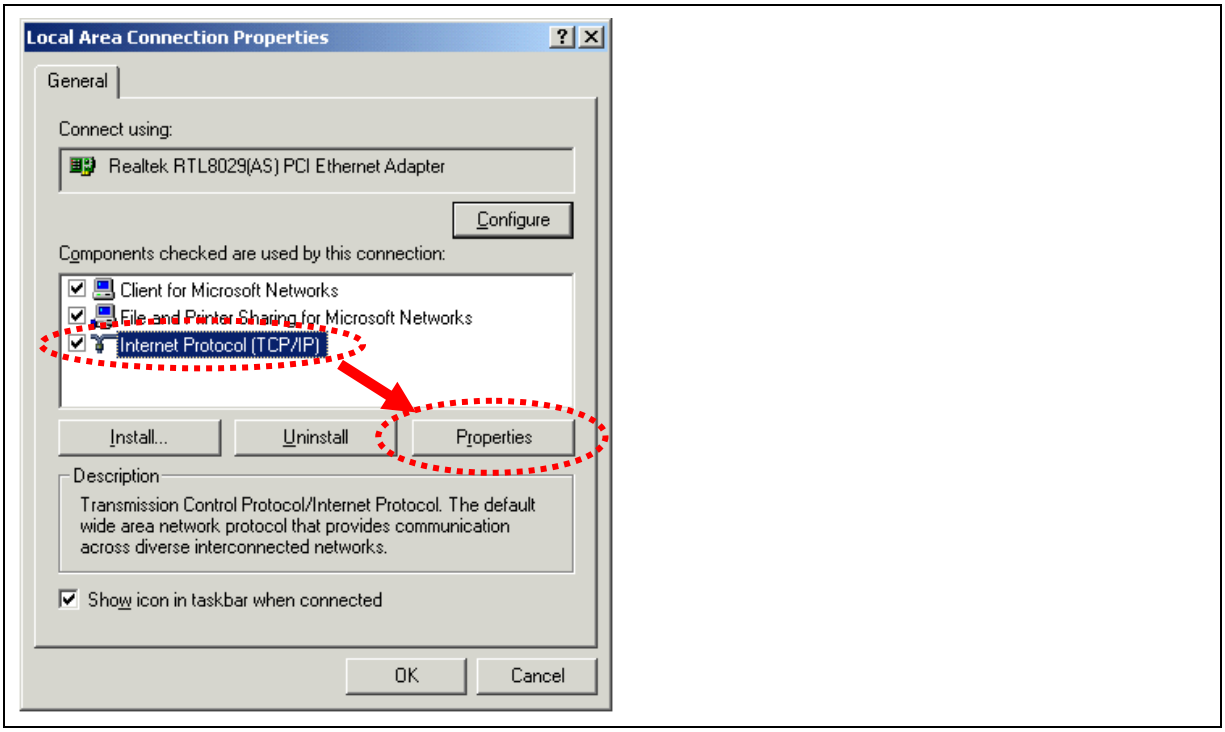


2. Select '**Obtain an IP address from a DHCP server**', and then click 'OK'.

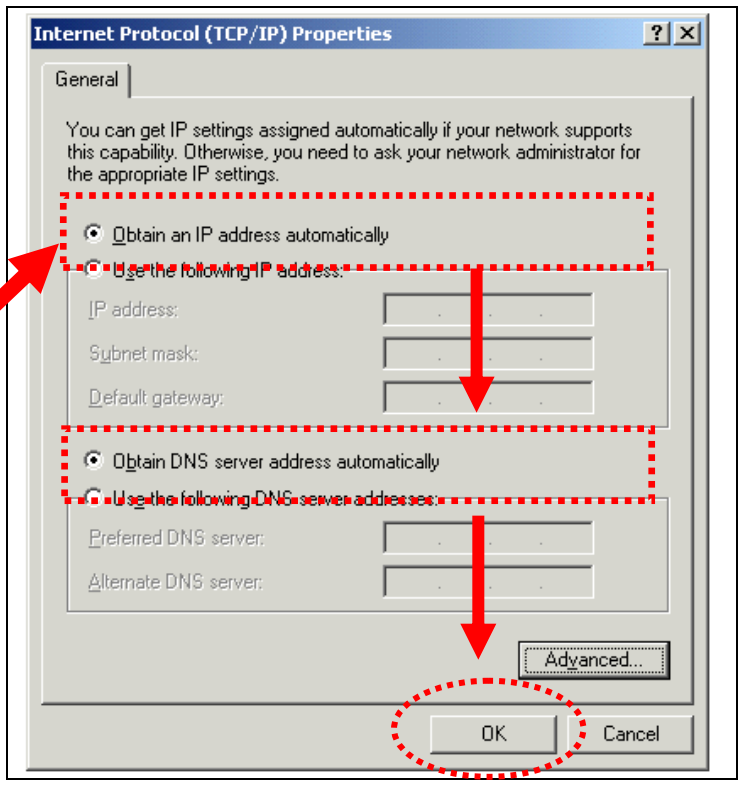

TCP/IP Properties
Bindings
Advanced
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address from a DHCP server
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

2.4.2 Windows 2000

1. Click '**Start**' button (it should be located at lower-left corner of your computer), then click control panel. Double-click ***Network and Dial-up Connections*** icon, double click ***Local Area Connection,*** and ***Local Area Connection Properties*** window will appear. Select '**Internet Protocol (TCP/IP)**', then click '**Properties**'.

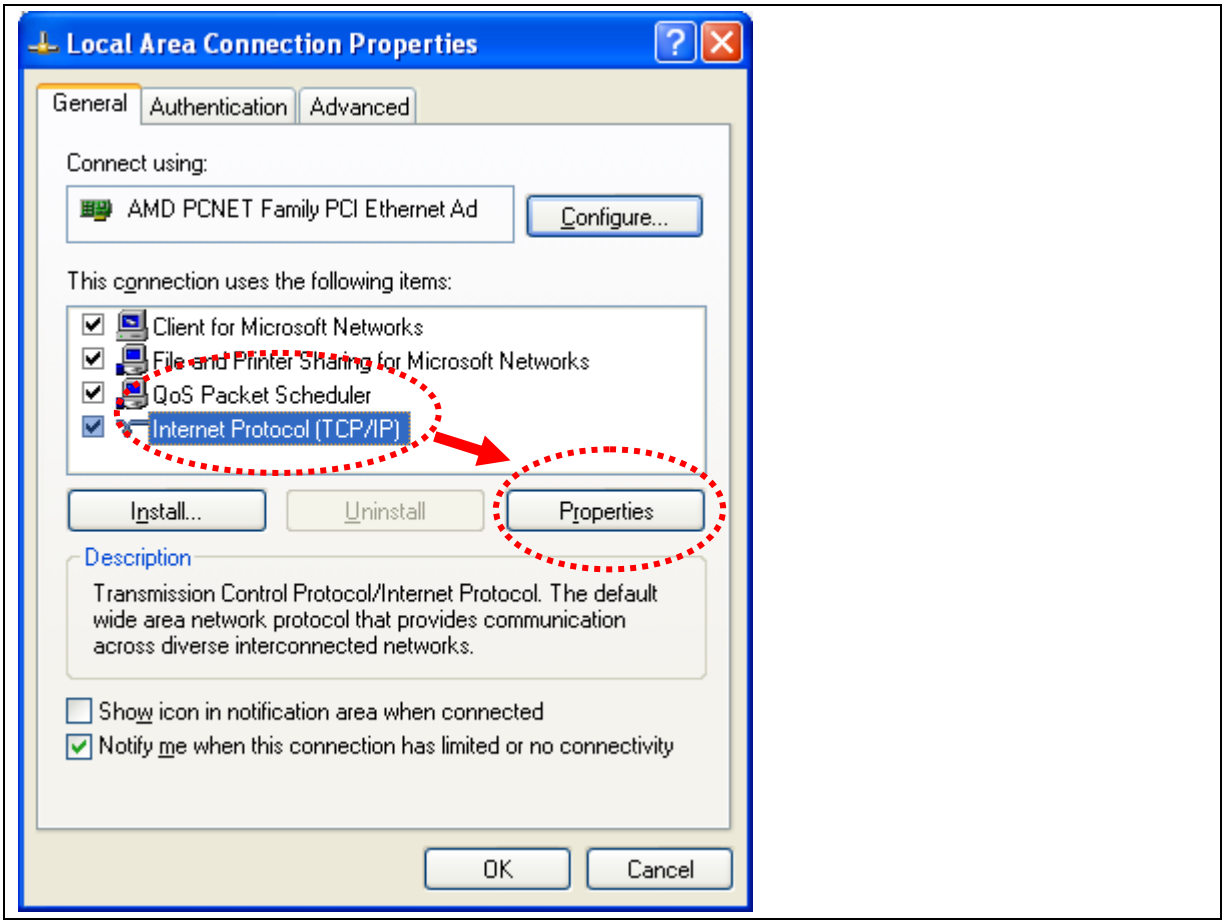


2. Select '**Obtain an IP address automatically**' and '**Obtain DNS server address automatically**', then click '**OK**'.

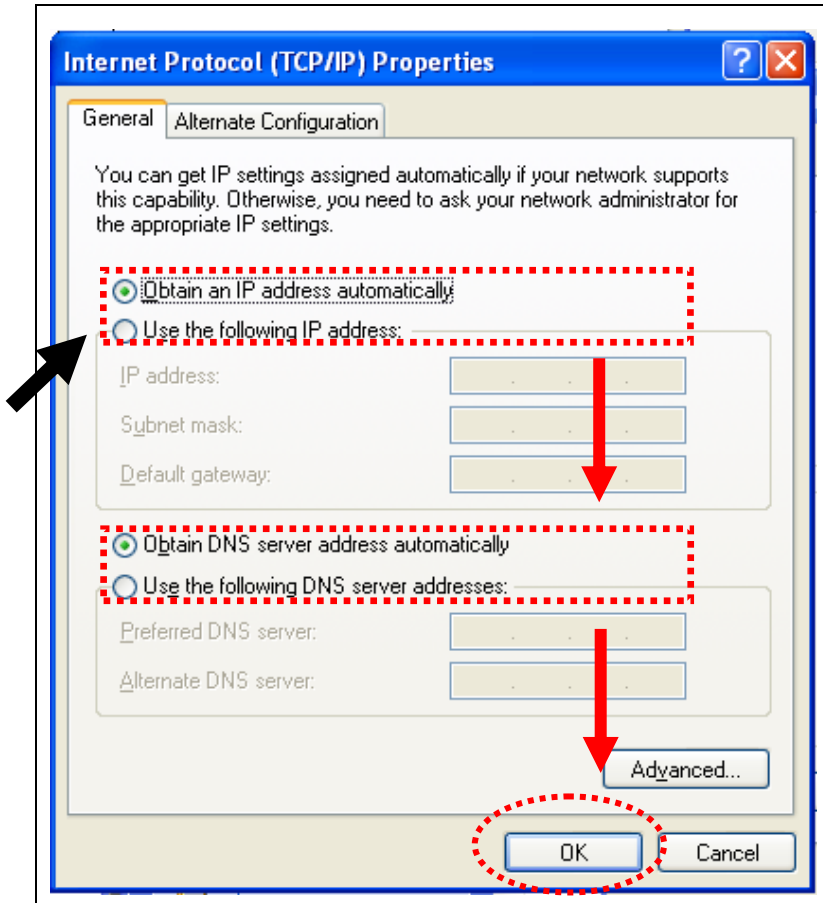

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

2.4.3 Windows XP

1. Click '**Start**' button (it should be located at lower-left corner of your computer), then click control panel. Double-click ***Network and Internet Connections*** icon, click ***Network Connections,*** then double-click ***Local Area Connection, Local Area Connection Status*** window will appear, and then click '**Properties**'.

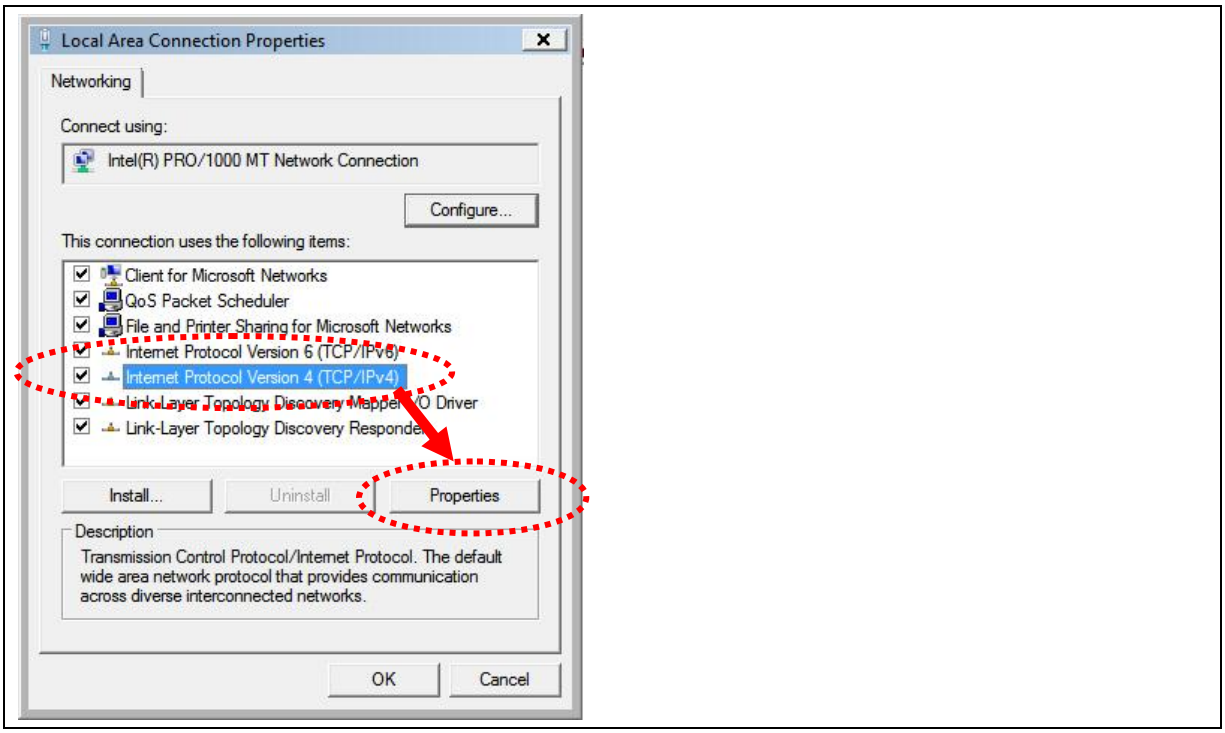


2. Select '**Obtain an IP address automatically**' and '**Obtain DNS server address automatically**', then click '**OK**'.

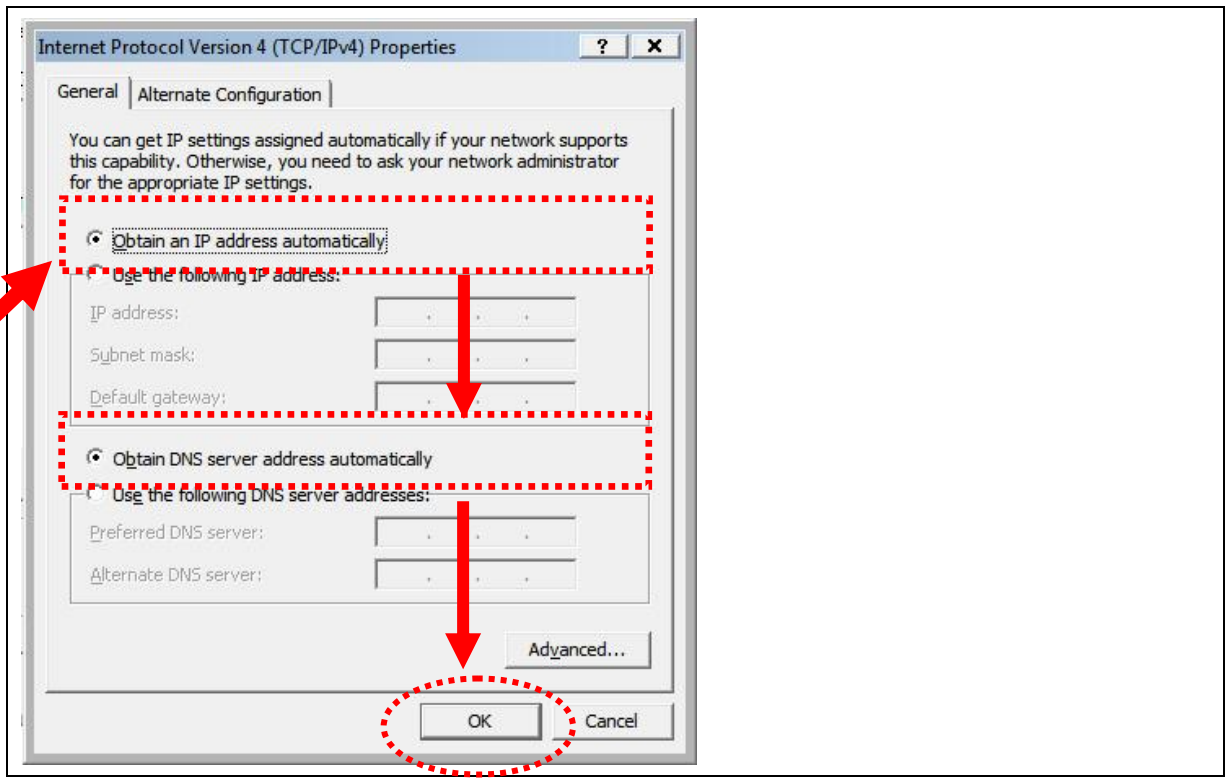

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

2.4.4 Windows Vista / Windows 7

1. Click '**Start**' button (it should be located at lower-left corner of your computer), then click control panel. Click ***View Network Status and Tasks***, and then click ***Manage Network Connections.*** Right-click ***Local Area Network, then select 'Properties'. Local Area Connection Properties*** window will appear, select '**Internet Protocol Version 4 (TCP / IPv4)**', and then click '**Properties**'.

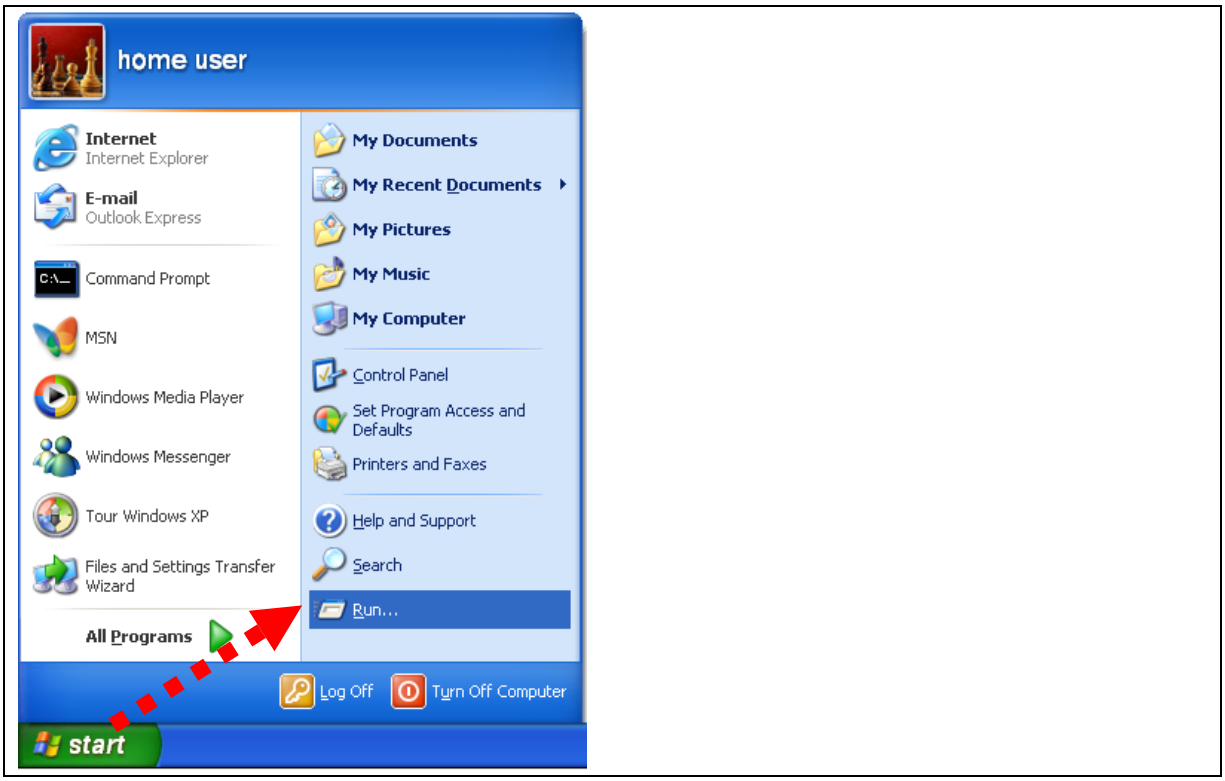


2. Select '**Obtain an IP address automatically**' and '**Obtain DNS server address automatically**', then click 'OK'.

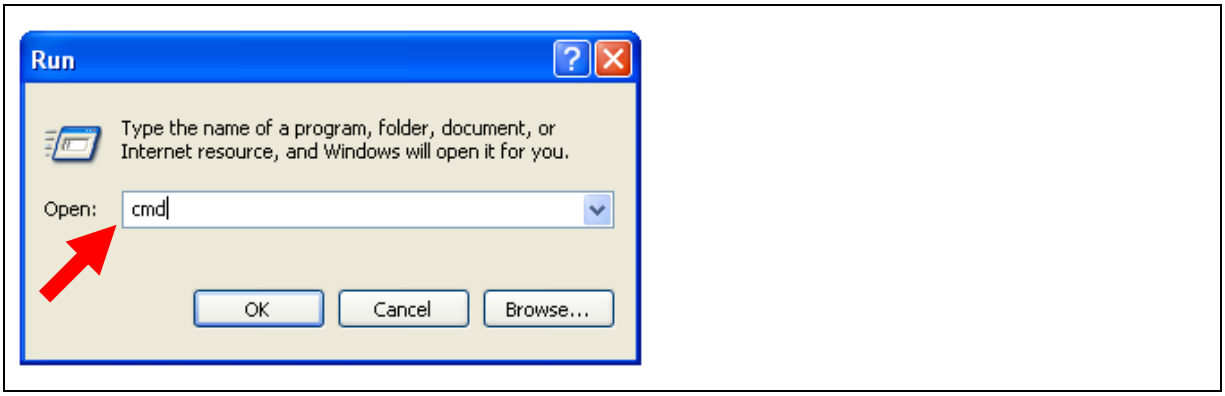

Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

2.4.5 Router IP Address Lookup

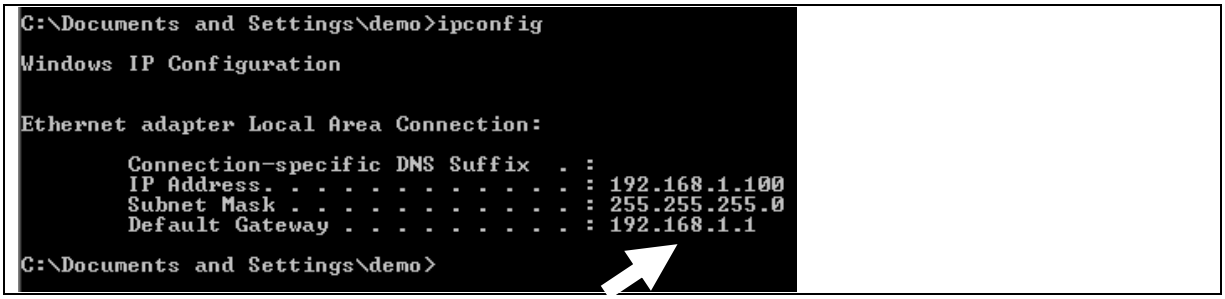
After the IP address setup was completed, please clicks '**Start**' → '**run**' at the bottom-lower corner of your desktop:



Input '**cmd**', and then click '**OK**'



Input '**ipconfig**', then press '**Enter**' key. Please check the IP address followed by '**Default Gateway**' (In this example, the gateway IP address of router is 192.168.1.1)

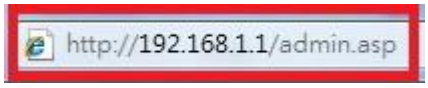

C:\Documents and Settings\demo>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.1.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\Documents and Settings\demo>

NOTE: If the IP address of Gateway is not displayed, or the address followed by 'IP Address' begins with '169.x.x.x', please recheck network connection between your computer and router, and / or go to the beginning of this chapter, to recheck every step of network setup procedure.

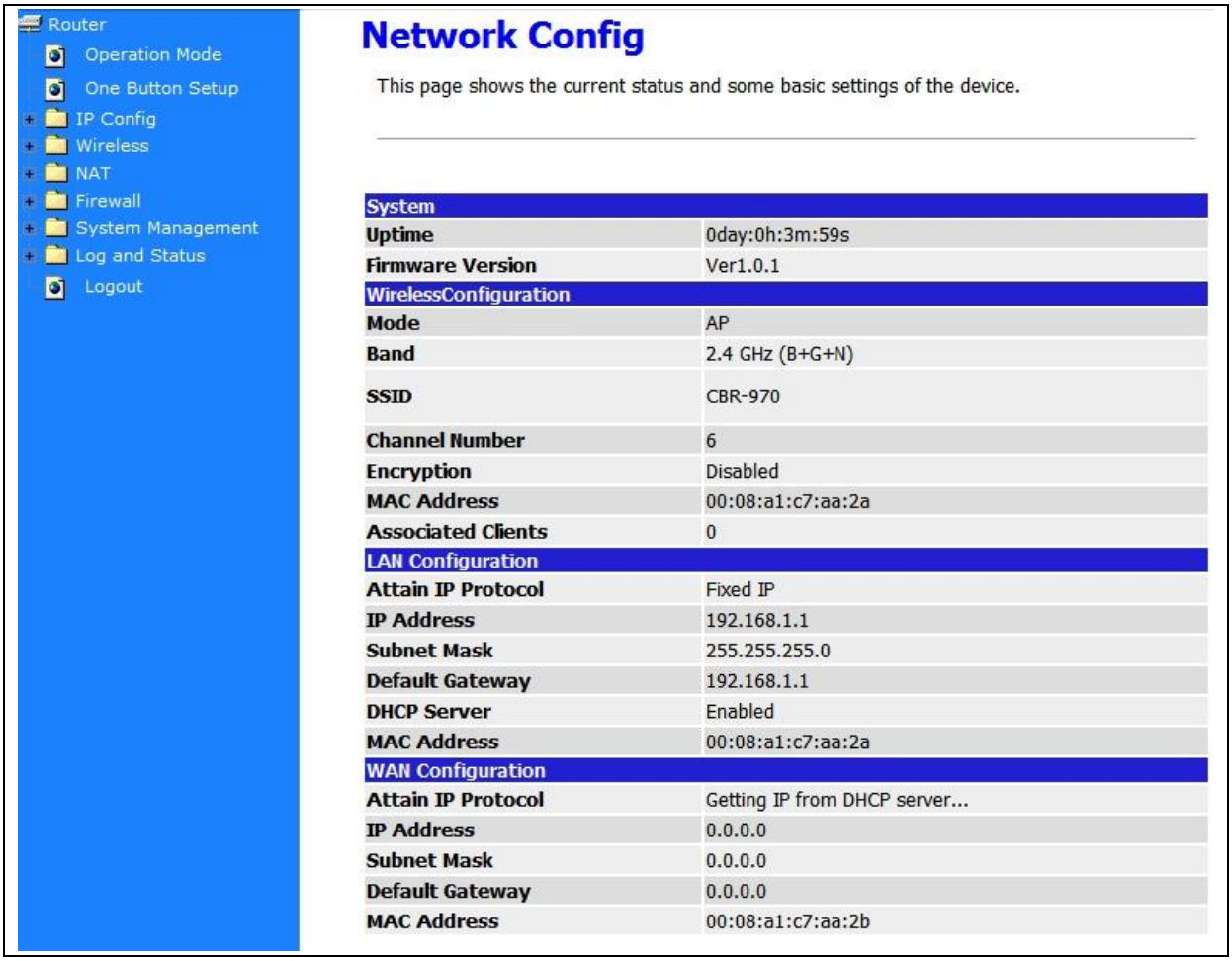
2.4.6 Connect the Wireless Router's management Interface by Web Browser

After your computer obtained an IP address from wireless router, please start your web browser, and input the IP address of the wireless router in address bar, and the following message should be shown. Please click "**Administrator**" to login the CBR-970/971.

Notes: The default IP of the wireless router is 192.168.1.1



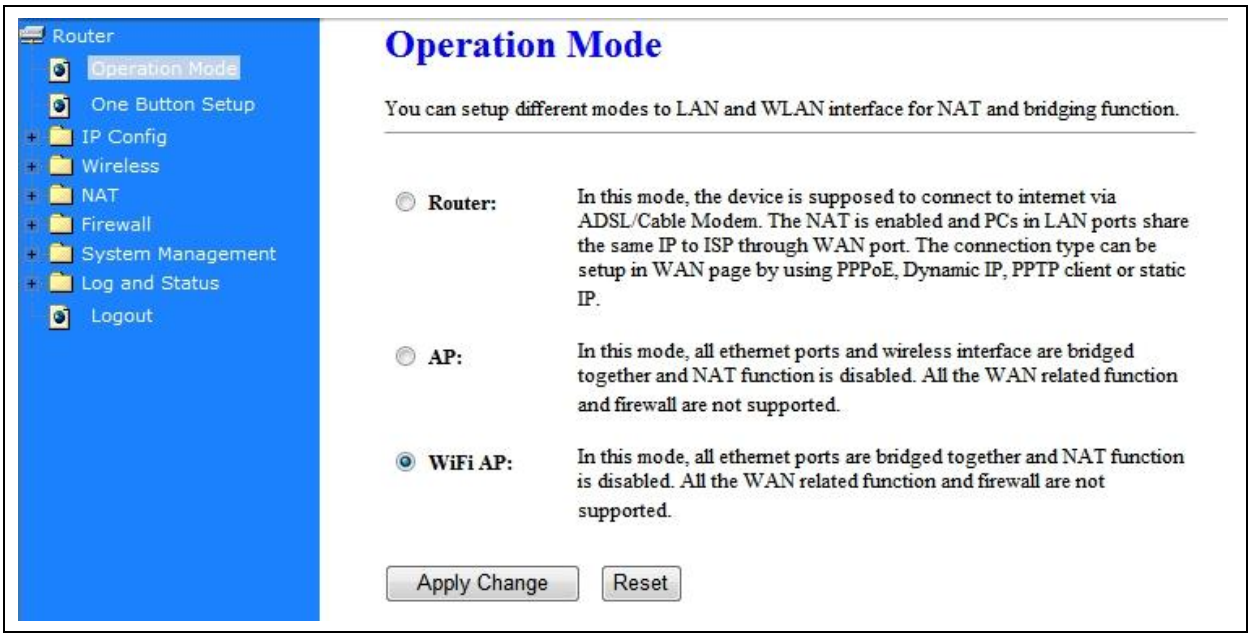
Please input user name and password in the field respectively. Default user name is '**admin**', and default password is '**admin**', then press '**Login**' button to login the web management interface of the wireless router.



NOTE: If you can't see the web management interface, and you're being prompted to input user name and password again, it means you didn't input username and password correctly. Please retype user name and password again. If you're certain about the user name and password what you type are correct, please go to 'Troubleshooting' to perform a factory reset, to set the password back to the default value.

Chapter 3 Operation Modes and One Button Setup

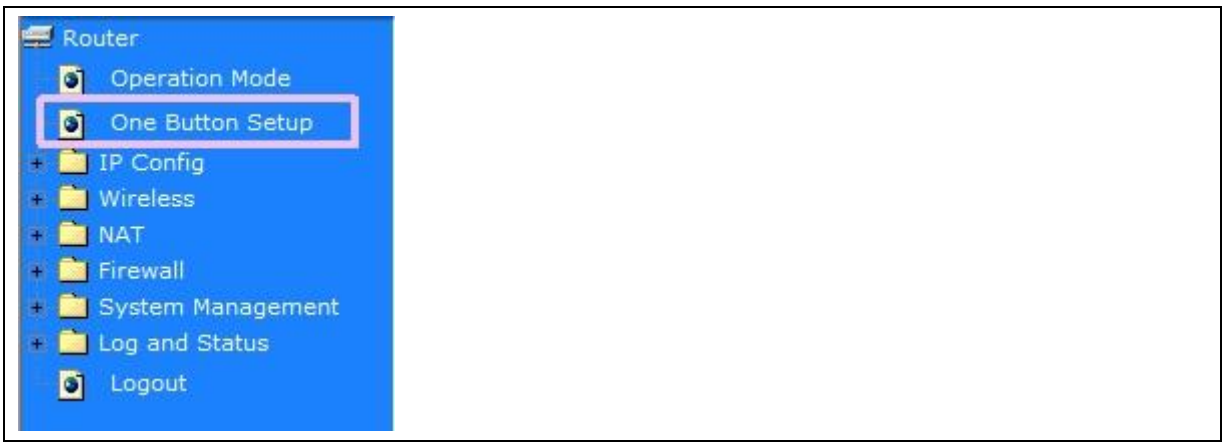
Before starting with the configurations you may select desired operation mode from "**Operation Mode**" in the left tree menu. Please refer to Chapter 2 for applications for each operation mode.

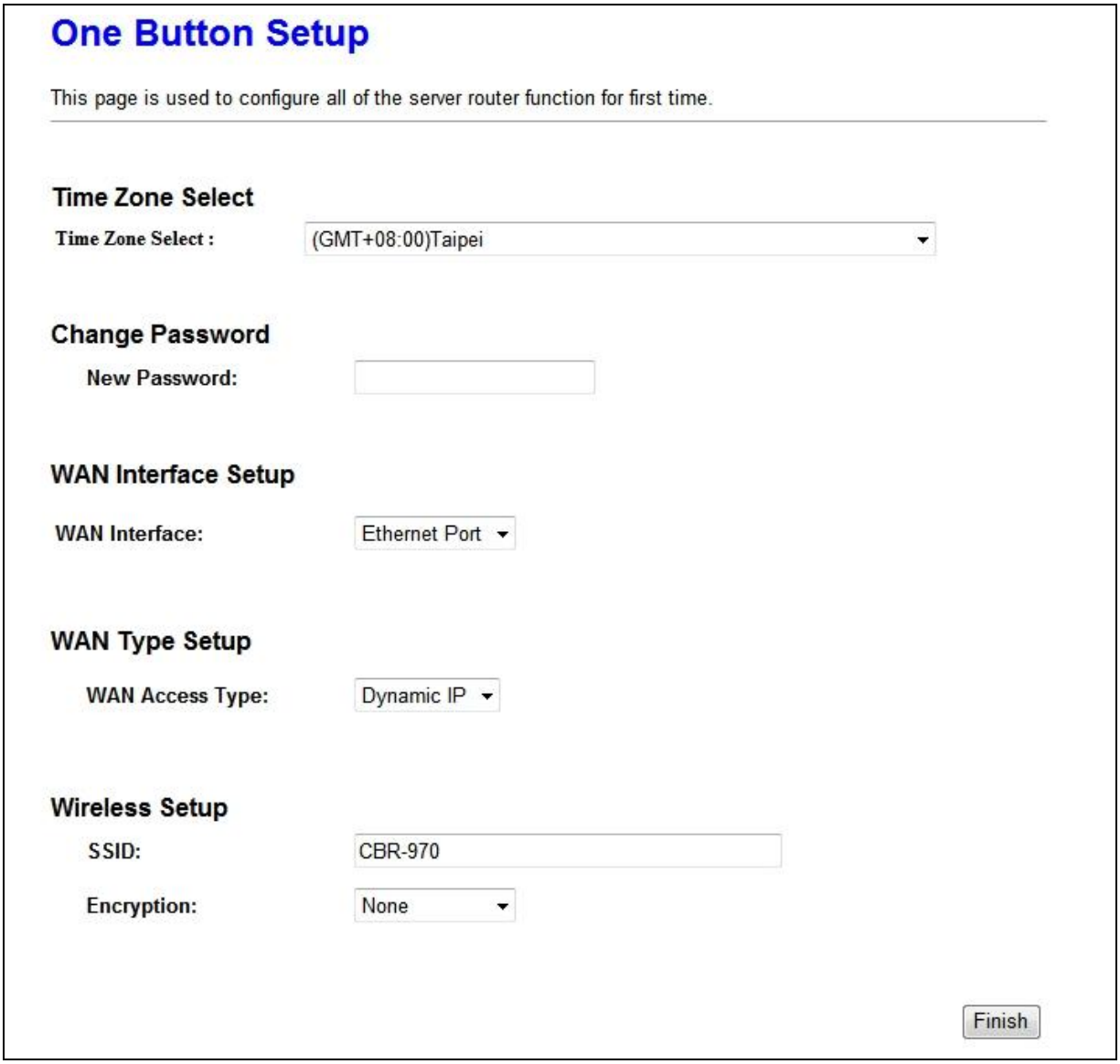

Router
Operation Mode
One Button Setup
IP Config
Wireless
NAT
Firewall
System Management
Log and Status
Logout
Operation Mode
You can setup different modes to LAN and WLAN interface for NAT and bridging function.
Router:
In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPoE, Dynamic IP, PPTP client or static IP.
AP:
In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
WiFi AP:
In this mode, all ethernet ports are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
Apply Change
Reset

Simply choose desired operation mode and click "**Apply Change**" and a step-by-step setup wizard sill guide you through the setup procedure.

CBR-970/971's "**One Button Setup**" will help you to setup the basic setting of the wireless router with simplified procedure. You do not need to learn much complicated network proper name but you still can setup the wireless router by yourself.

Please click "**One Button Setup"** function, and then click the "finish" to complete the setting. The router will reboot automatically.





Item	Description
Time Zone Select	Press button to choose a time zone of the location you live from the drop-down list.
Change Password	Input new password here
Device Name	Input new device name here
WAN Interface Setup	Choose the broadband interface you are using. The wireless router supports Ethernet Port / Wireless / 3.5G / WiMAX 4 different types of interface. Please refer to Chapter 4.1.1 for details about all WAN type settings.
Wireless Setup	Configure Wireless SSID and Security.
Finish	Click finish button to complete the setting

Chapter 4 Router Mode Advanced Configuration

This chapter describes how to setup the access the router through the web browser. Please be noted that in order to access the router's admin page, a computer must be connected to one of the LAN ports on the router. The WLAN Broadband Router is delivered with the following factory default parameters on the Ethernet LAN interfaces.

Default IP Address: 192.168.1.1

Default IP subnet mask: 255.255.255.0

WEB login User Name: admin

WEB login Password: admin

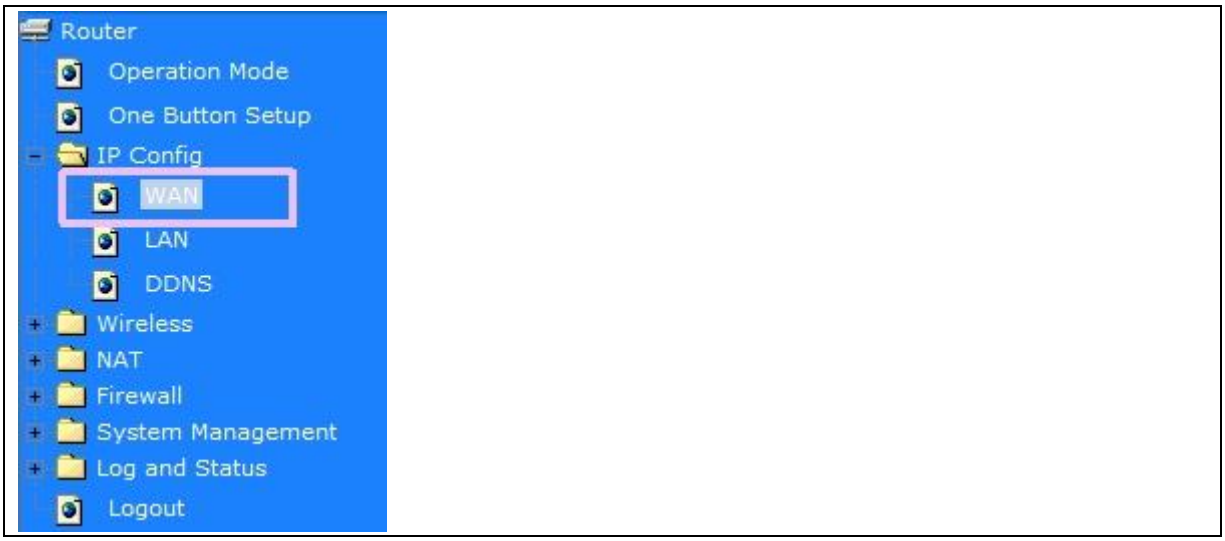
4.1 IP Configuration

In this section that user could configure the connection type of WAN port. Please check with your Internet Service Provider about the essential connection parameter.

4.1.1 WAN Interface Setup

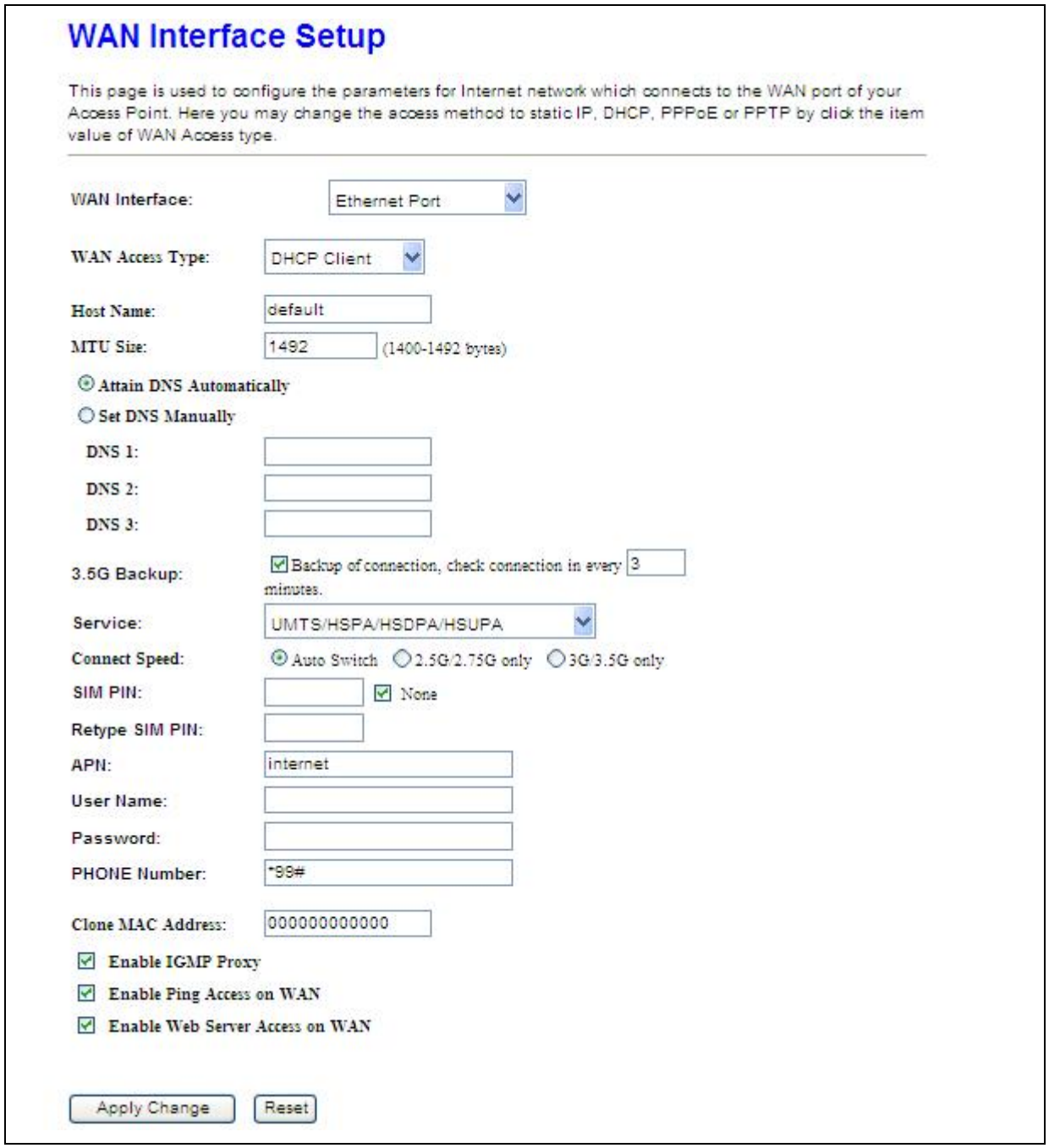
Select **WAN** under the **IP Config** menu. CBR-970/971 supports 4 interfaces and 5 access types. Follow the instructions below for each to set up accordingly.

Choose your WAN Interface and WAN type, and click **Next,** its associated settings will show up.



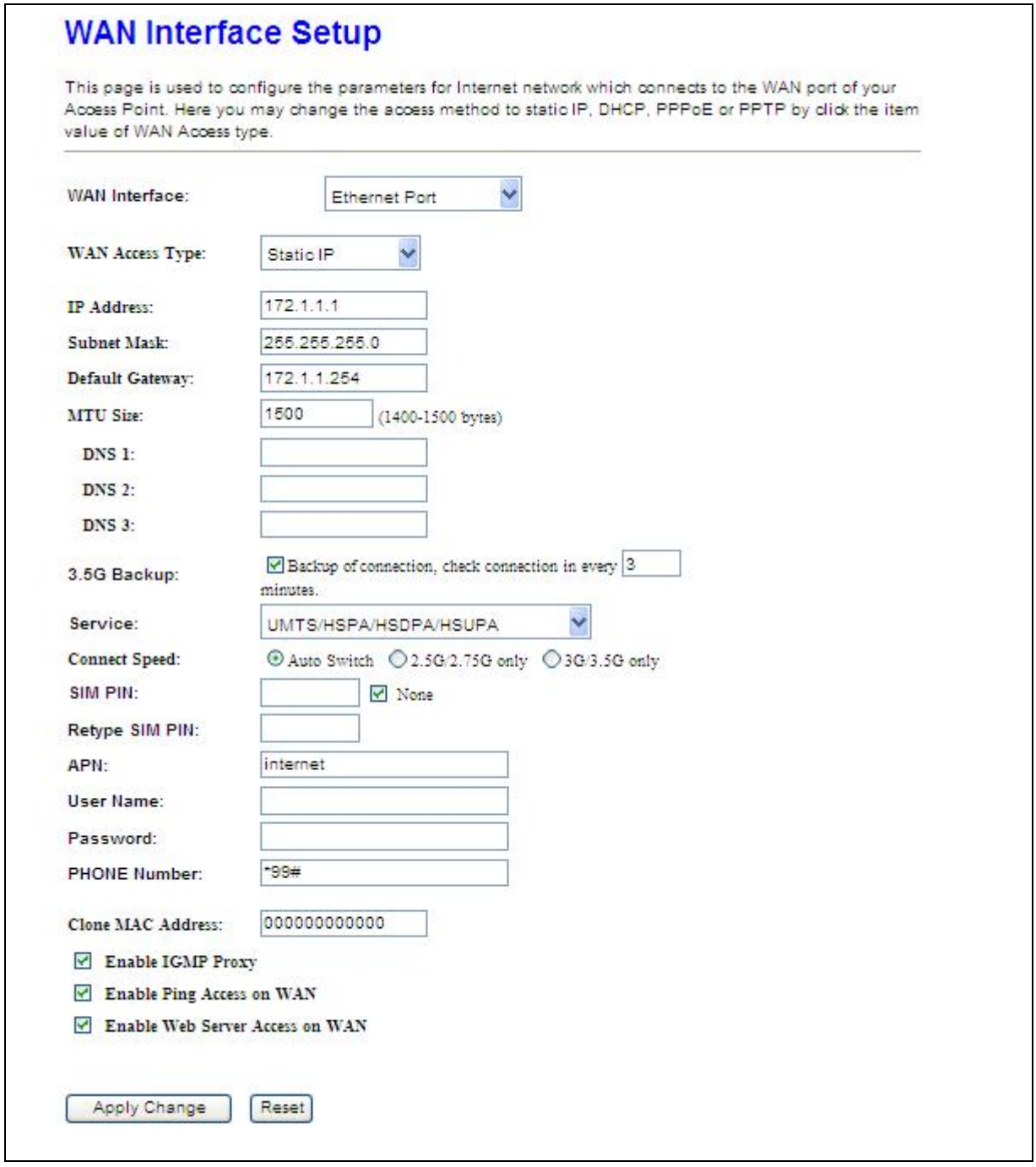
4.1.1.1 WAN Interface – Ethernet Port

If you are using an Ethernet cable to connect the Internet, please select **Ethernet port**.


WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.
WAN Interface: Ethernet Port
WAN Access Type: DHCP Client
Host Name: default
MTU Size: 1492 (1400-1492 bytes)
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
3.5G Backup: Backup of connection, check connection in every 3 minutes.
Service: UMTS/HSPA/HSDPA/HSUPA
Connect Speed: Auto Switch 2.5G/2.75G only 3G/3.5G only
SIM PIN: None
Retype SIM PIN:
APN: internet
User Name:
Password:
PHONE Number: *99#
Clone MAC Address: 000000000000
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Apply Change
Reset

4.1.1.1.1 WAN Access Type – Static IP

If you applied for a **Static IP** connection type from ISP, please follow the steps to set up your WAN connection.



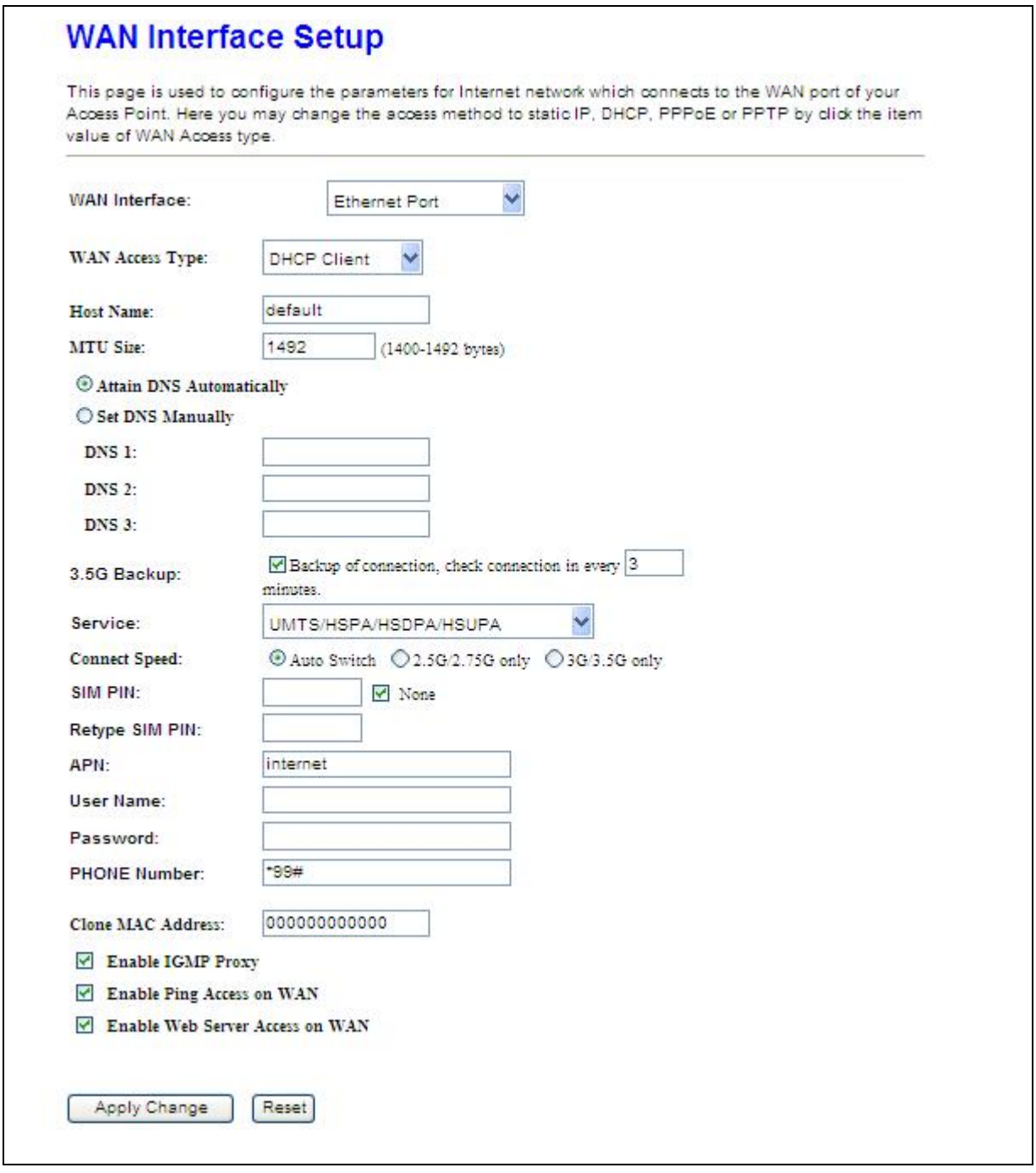
Item	Description
IP Address	Please enter the IP address which is provided by your ISP. If you don't have it, please contact your ISP.
Subnet Mask	Please enter the Subnet Mask address.

Default Gateway	Input ISP Default Gateway Address. If you don't know, please check with your ISP.
MTU Size	The term **Maximum transmission unit** refers to the size (in bytes) of the largest PDU that a given layer of a communications protocol can pass onwards. Users can improve network efficiency by adjusting the value of MTU. Most of OS will give users a default value which is fit for most of users. Users can modify this value also. Please enter value, max number is 1500 bytes.
DNS	If ISP provides DNS information, please select **Attain DNS automatically**. Or you should select **Set DNS Manually**, and then input the DNS address.
3.5G Backup	Check this option to allow failover Internet connection support with 3.5G. By default the router checks the connectivity every 3 minutes, if the connection fails then the router will attempt to establish a 3.5G connection for backup purpose.
Service	Select service type. (HSDPA/CDMA2000/TD-SCDMA).
Connect Speed	Select Preferred 2G/3G/3.5G connection speed.
SIM PIN / Retype SIM PIN	Enter the PIN code of your SIM card here.
APN	Enter the Access Point Number provided by your ISP, default setting is **internet**.
Username / Password	Enter the username/password required for establishing the 3.5G connection.
PHONE number	Enter the dialing number, default setting is ***99#**.
Clone MAC	If your ISP asks you to enter a specific MAC Address, please input the correct info at the column.
Enable IGMP Proxy	The **Internet Group Management Protocol** (**IGMP**) is a communication protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable **IGMP Proxy** to provide service.
Enable Ping Access on WAN	To enable WAN ICMP response.

Enable Web Server Access on WAN	Enable Web Server Access function from WAN side.
Apply Change & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

4.1.1.1.2 WAN Access -- Dynamic IP

If your WAN access type is **Dynamic IP**, please complete the settings as following instructions.



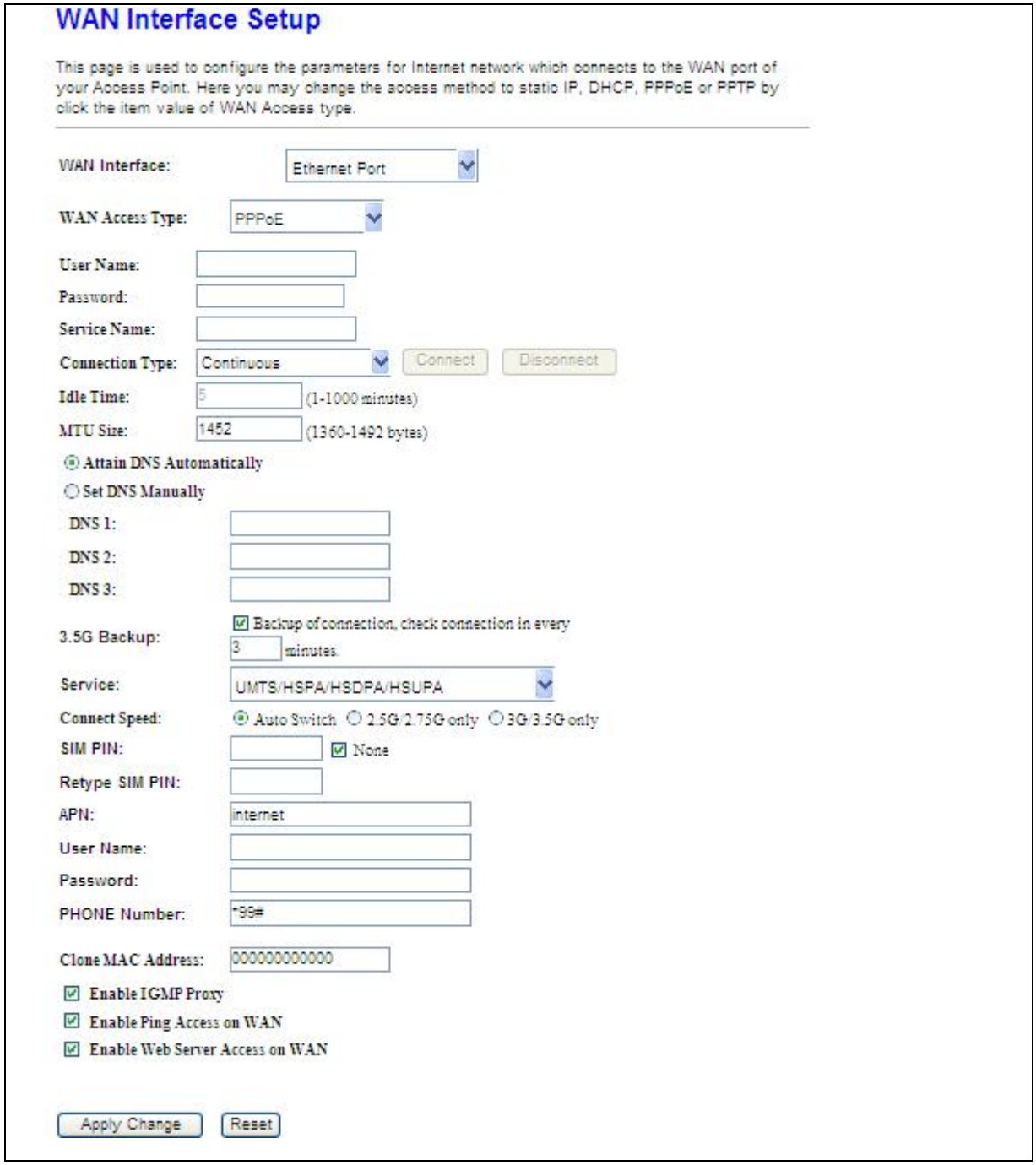
Item	Description
Host Name	The host name is optional; but if your ISP requires you to input a specific host name, please put it in, for example, 11n Broadband Router applied from ISP. Generally, Cable Modem

	will provide the hostname information.
MTU Size	MTU stands for Maximum Transmission Unit. For Static IP connection, the default MTU should be provided by computer operating systems (OS). Advanced users can set the MTU manually for increasing the internet performance. The largest number is 1492 byte
DNS	If ISP provides you DNS information, please select **Attain DNS automatically,** otherwise select **Set DNS Manually** and input the DNS information into the blank.
3.5G Backup	Check this option to allow failover Internet connection support with 3.5G. By default the router checks the connectivity every 3 minutes, if the connection fails then the router will attempt to establish a 3.5G connection for backup purpose.
Service	Select service type. (HSDPA/CDMA2000/TD-SCDMA).
Connect Speed	Select Preferred 2G/3G/3.5G connection speed.
SIM PIN / Retype SIM PIN	Enter the PIN code of your SIM card here.
APN	Enter the Access Point Number provided by your ISP, default setting is **internet**.
Username / Password	Enter the username/password required for establishing the 3.5G connection.
PHONE number	Enter the dialing number, default setting is ***99#**.
Clone MAC Address	Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.
Enable IGMP Proxy	The **Internet Group Management Protocol (IGMP)** is a communication protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable **IGMP Proxy** to provide service.
Enable Ping Access on WAN	Select **Enable Ping Access on WAN**, will make WAN IP address response to any ping request from Internet users. It is a common way for hacker to ping public WAN IP address, to

	see is there any WAN IP address available.
Enable Web Server Access on WAN	This option is to enable Web Server Access function on WAN.
Apply Change & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

4.1.1.1.3 WAN Access Type -- PPPoE

If you applied for a **PPPoE** connection type from ISP, please follow the steps to set up your WAN connection.



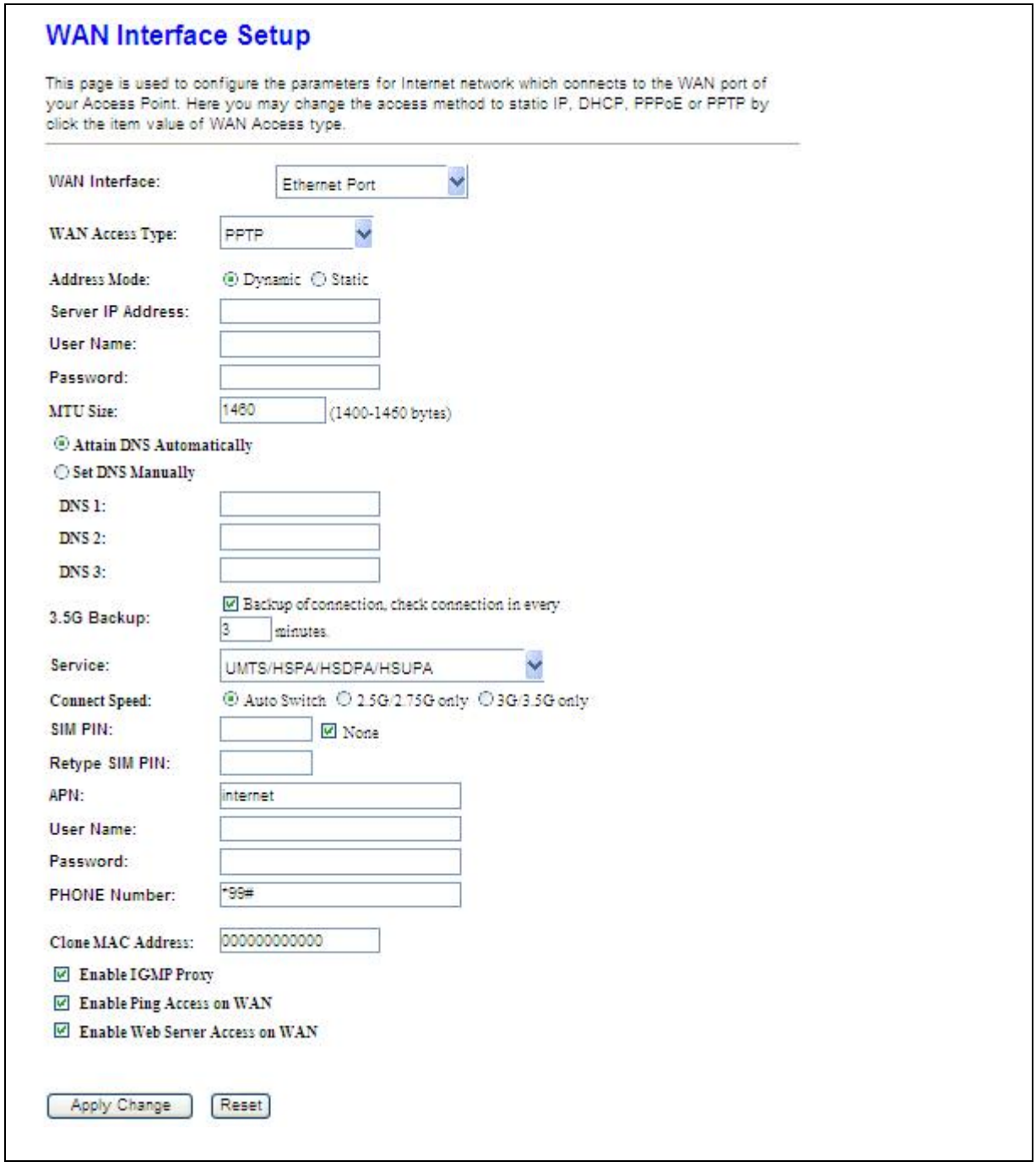
Item	Description
User Name	Input your user name supplied by ISP. If you don't know, please check with your ISP.

Password	Input your Password supplied by ISP
Service Name	Input the service name supplied by ISP.
Connection Type	It has three types: **Continuous, Connect on Demand,** and **Manual.**
Idle Time	It is the time of inactivity before disconnecting your PPPoE session. Enter an Idle Time (in minutes) to define a maximum period of time for which the Internet connect is maintained during inactivity. If the connection is inactive for longer than the defined Idle Time, then the connection will be dropped. Either set this to zero or enable Auto-reconnect to disable this feature.
MTU Size	MTU stands for Maximum Transmission Unit. For PPPoE connection, the default MTU should be provided by computer operating systems (OS). Advanced users can set the MTU manually for increasing the internet performance. The largest number allowed by Ethernet at the network layer is 1492 byte
DNS	If ISP provides you DNS information, please select **Attain DNS automatically,** otherwise select **Set DNS Manually** and input the DNS information into the blank.
3.5G Backup	Check this option to allow failover Internet connection support with 3.5G. By default the router checks the connectivity every 3 minutes, if the connection fails then the router will attempt to establish a 3.5G connection for backup purpose.
Service	Select service type. (HSDPA/CDMA2000/TD-SCDMA).
Connect Speed	Select Preferred 2G/3G/3.5G connection speed.
SIM PIN / Retype SIM PIN	Enter the PIN code of your SIM card here.
APN	Enter the Access Point Number provided by your ISP,

	default setting is **internet**.
Username / Password	Enter the username/password required for establishing the 3.5G connection.
PHONE number	Enter the dialing number, default setting is ***99#**.
Clone MAC Address	Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.
Enable IGMP Proxy	The **Internet Group Management Protocol (IGMP)** is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable **IGMP Proxy** to provide service.
Enable Ping Access on WAN	Select **Enable Ping Access on WAN**, will make WAN IP address response to any ping request from Internet users. It is a common way for hacker to ping public WAN IP address, to see is there any WAN IP address available.
Enable Web Server Access on WAN	This option is to enable **Web Server Access** function on WAN.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

4.1.1.1.4 WAN Access Type -- PPTP

If you have applied for a **PPTP** connection type from ISP, please follow the steps to set up your WAN connection.



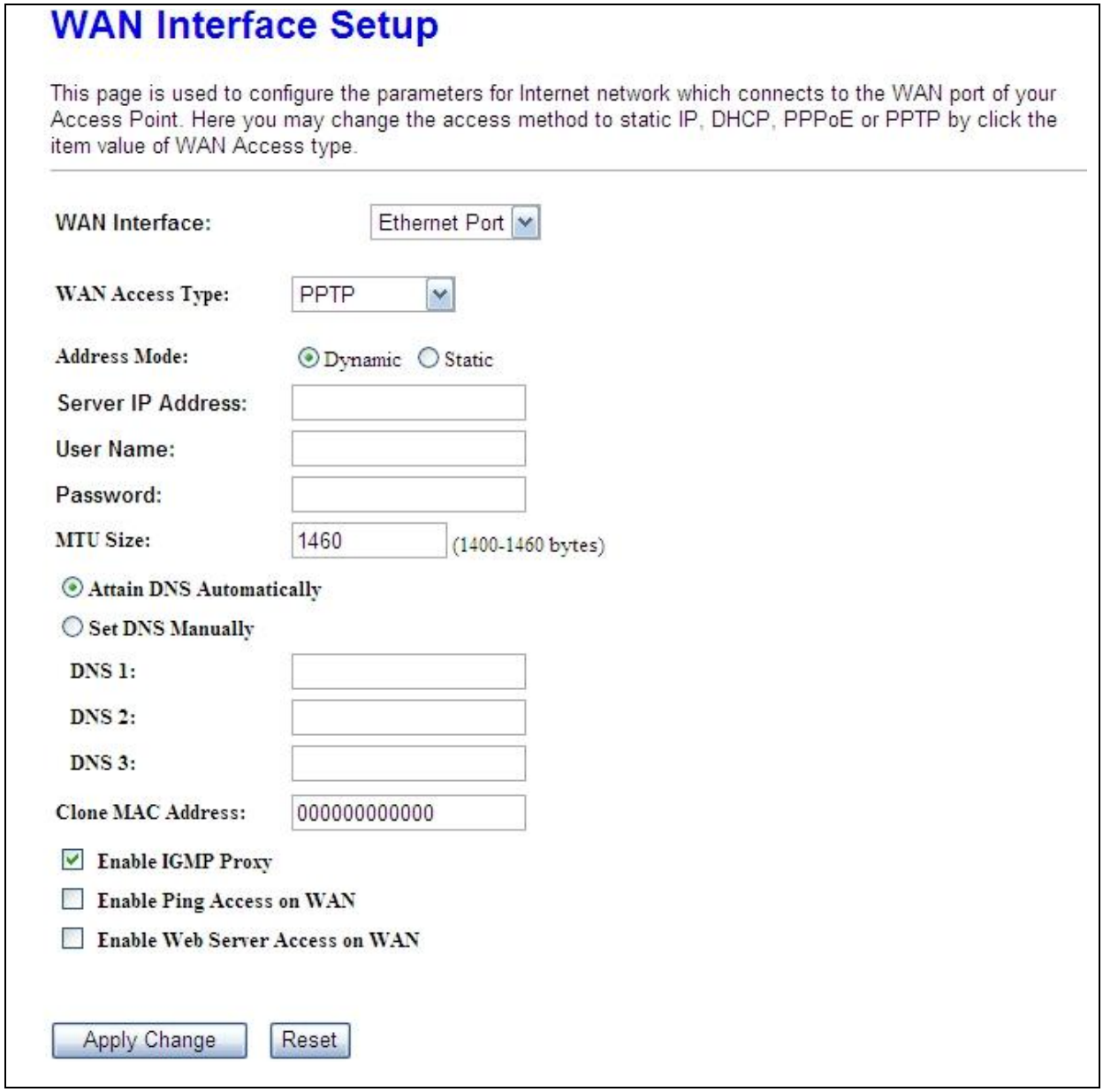
Item	Description
IP Address	Input your IP Address supplied by ISP. If you don't know, please check with your ISP.

Subnet Mask	Input Subnet Mask, normally it is **255.255.255.0.**
Server IP Address	Input your Server IP Address supplied by ISP. If you don't know, please check with your ISP.
User Name	Input the PPTP Account supplied by ISP, for example. If you don't know, please check with your ISP.
Password	Input the Password supplied by ISP.
MTU	MTU stands for Maximum Transmission Unit. For PPPoE connection, the default MTU should be provided by computer operating systems (OS). Advanced users can set the MTU manually for increasing the internet performance. The largest number allowed is 1460 byte
Request MPPPE Encryption	**Microsoft Point-to-Point Encryption (MPPE)** encrypts data in Point-to-Point Protocol (PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections. 128-bit key (strong), 56-bit key, and 40-bit key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.
DNS	If ISP provides you DNS information, please select **Attain DNS automatically**, otherwise select **Set DNS Manually** and input the DNS information into the blank.
3.5G Backup	Check this option to allow failover Internet connection support with 3.5G. By default the router checks the connectivity every 3 minutes, if the connection fails then the router will attempt to establish a 3.5G connection for backup purpose.
Service	Select service type. (HSDPA/CDMA2000/TD-SCDMA).
Connect Speed	Select Preferred 2G/3G/3.5G connection speed.

SIM PIN / Retype SIM PIN	Enter the PIN code of your SIM card here.
APN	Enter the Access Point Number provided by your ISP, default setting is **internet**.
Username / Password	Enter the username/password required for establishing the 3.5G connection.
PHONE number	Enter the dialing number, default setting is ***99#**.
Clone MAC Address	Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.
Enable IGMP Proxy	The **Internet Group Management Protocol (IGMP)** is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable **IGMP Proxy** to provide service.
Enable Ping Access on WAN	Select **Enable Ping Access on WAN**, will make WAN IP address response to any ping request from Internet users. It is a common way for hacker to ping public WAN IP address, to see is there any WAN IP address available.
Enable Web Server Access on WAN	This option is to enable **Web Server Access** function on WAN.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

4.1.1.1.5 WAN Access Type – L2TP

If you have applied for a **PPTP** connection type from ISP, please follow the steps to set up your WAN connection.



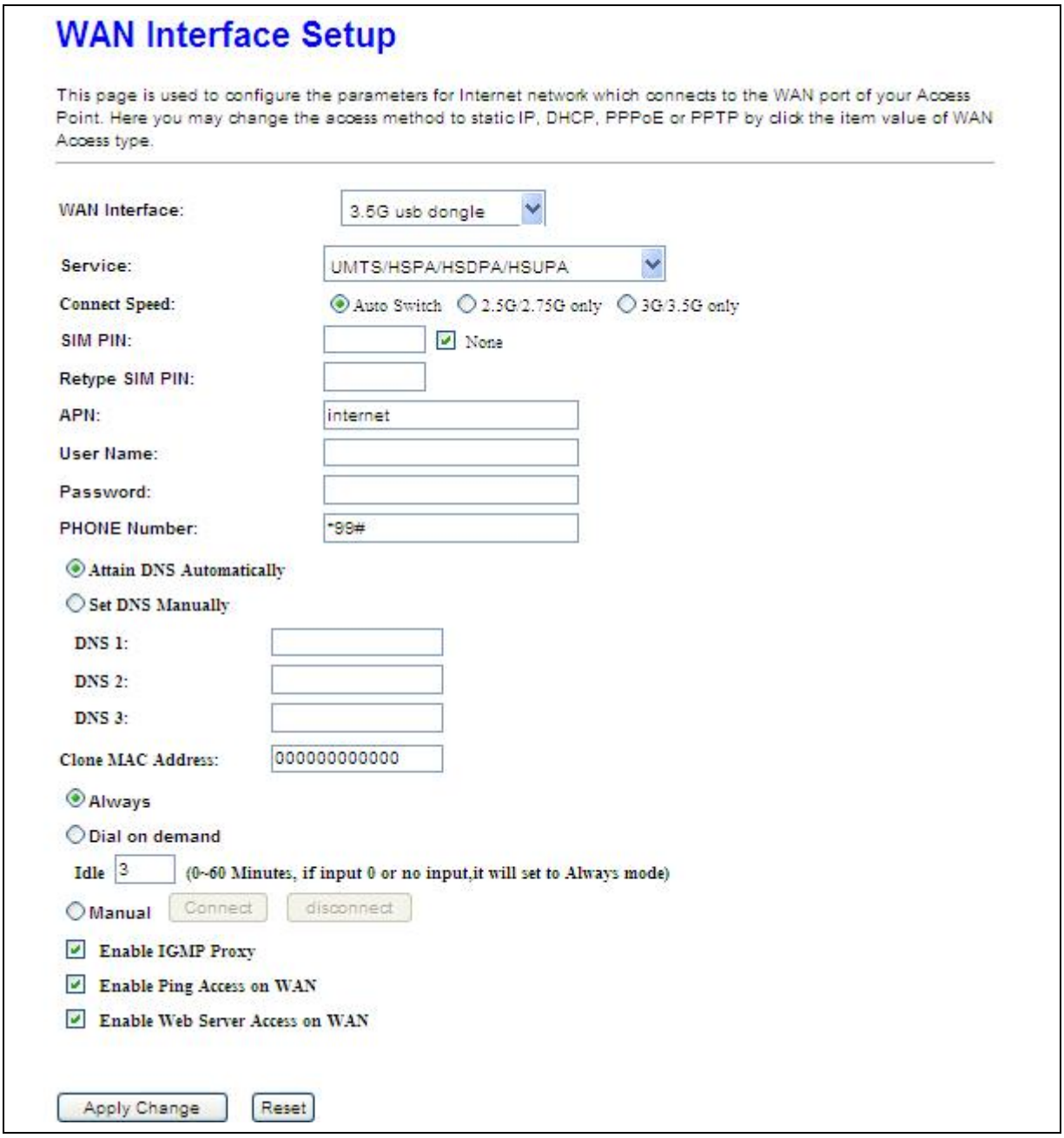
Item	Description
IP Address	Input your IP Address supplied by ISP. If you don't know, please check with your ISP.
Subnet Mask	Input Subnet Mask, normally it is **255.255.255.0.**
Server IP Address	Input your Server IP Address supplied by ISP. If you

	don’t know, please check with your ISP.
User Name	Input the PPTP Account supplied by ISP, for example. If you don’t know, please check with your ISP.
Password	Input the Password supplied by ISP.
MTU	MTU stands for Maximum Transmission Unit. For PPPoE connection, the default MTU should be provided by computer operating systems (OS). Advanced users can set the MTU manually for increasing the internet performance. The largest number allowed is 1460 byte
Request MPPPE Encryption	**Microsoft Point-to-Point Encryption (MPPE)** encrypts data in Point-to-Point Protocol (PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections. 128-bit key (strong), 56-bit key, and 40-bit key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.
DNS	If ISP provides you DNS information, please select **Attain DNS automatically**, otherwise select **Set DNS Manually** and input the DNS information into the blank.
3.5G Backup	Check this option to allow failover Internet connection support with 3.5G. By default the router checks the connectivity every 3 minutes, if the connection fails then the router will attempt to establish a 3.5G connection for backup purpose.
Service	Select service type. (HSDPA/CDMA2000/TD-SCDMA).
Connect Speed	Select Preferred 2G/3G/3.5G connection speed.
SIM PIN / Retype SIM PIN	Enter the PIN code of your SIM card here.
APN	Enter the Access Point Number provided by your ISP,

	default setting is **internet**.
Username / Password	Enter the username/password required for establishing the 3.5G connection.
PHONE number	Enter the dialing number, default setting is ***99#**.
Clone MAC Address	Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.
Enable IGMP Proxy	The **Internet Group Management Protocol (IGMP)** is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable **IGMP Proxy** to provide service.
Enable Ping Access on WAN	Select **Enable Ping Access on WAN**, will make WAN IP address response to any ping request from Internet users. It is a common way for hacker to ping public WAN IP address, to see is there any WAN IP address available.
Enable Web Server Access on WAN	This option is to enable **Web Server Access** function on WAN.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

4.1.1.2 WAN Interface – 3.5G (HSDPA/UMTS) (CBR-971 only)

If you are using HSDPA/UMTS (3.5G connection) as the WAN Type, please select **3.5G USB Dongle** and fill in the required information as follows to directly access Internet via connected 3.5G adapter. At this moment, **Backup of Connection** is not available. When 3.5G signal cannot be reached, the system starts to search downward for 3/2.75/2.5G signals until none existed.

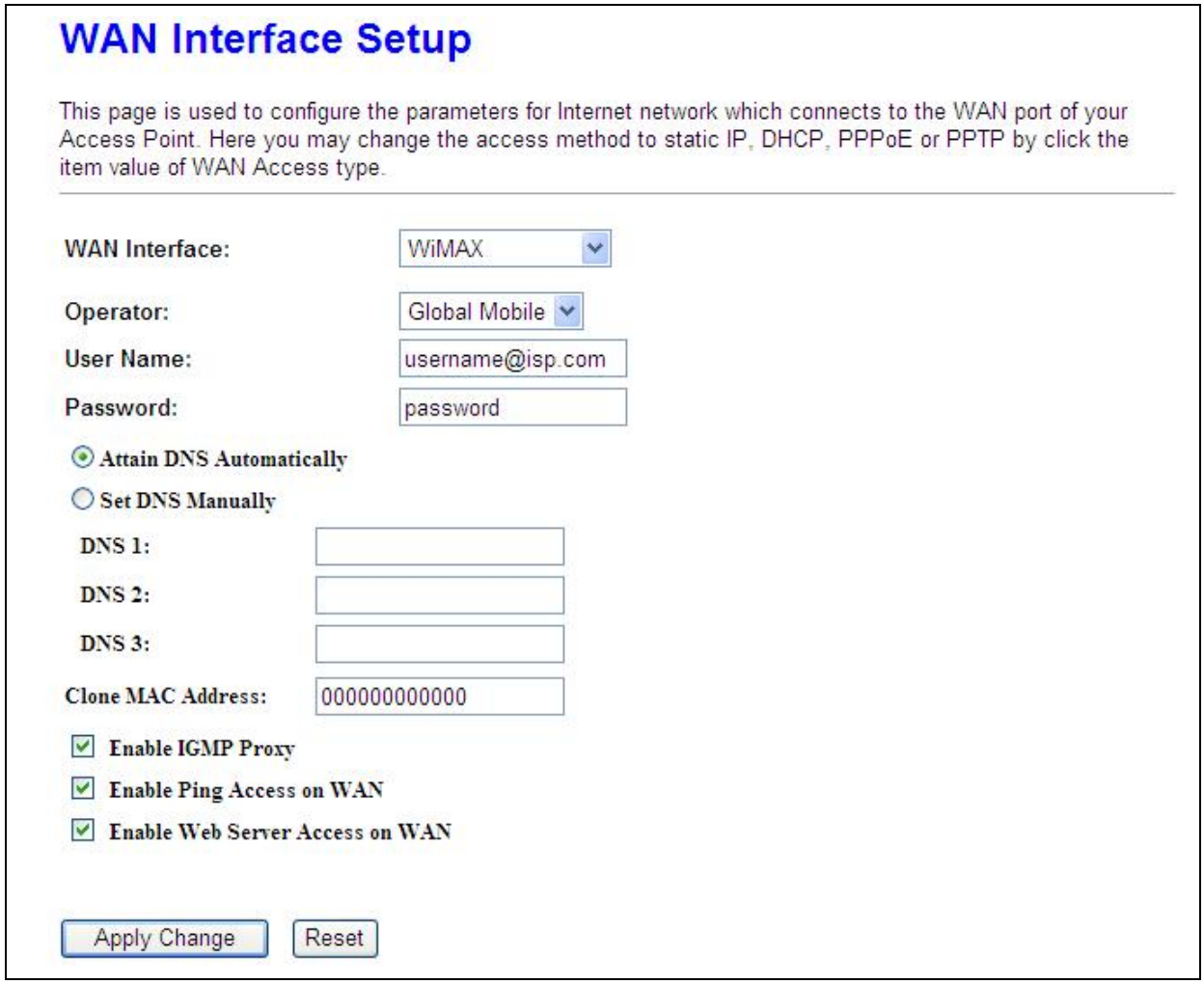


Item	Description
Service	Select correspond mobile connection service type.
Connection Speed	Select preferred mobile Internet connection speed.
SIM PIN	Enter the PIN code of your SIM card here.
Retype SIM PIN	Confirm your PIN code.
APN	Enter the Access Point Number provided by your ISP. Default is **internet**.
Username	Username/Password required for establishing the Internet connection.
Password	
PHONE Number	Enter the dialing number here, default setting is ***99#**.
DNS	If ISP provides you DNS information, please select **Attain DNS automatically,** otherwise select **Set DNS Manually** and input the DNS information into the blank.
Clone MAC Address	Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.
Always	Select Always for the 3.5G connection to be always established.
Dial on demand	Select Dial on demand to establish 3.5G connection only when there is an outgoing traffic.
Manual	Select Manual to manually connect or disconnect the 3.5G connection.
Enable IGMP Proxy	The **Internet Group Management Protocol (IGMP)** is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable **IGMP Proxy** to provide service.
Enable Ping Access on WAN	Select **Enable Ping Access on WAN**, will make WAN IP address response to any ping request from Internet

	users. It is a common way for hacker to ping public WAN IP address, to see is there any WAN IP address available.
Enable Web Server Access on WAN	This option is to enable **Web Server Access** function on WAN.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

4.1.1.3 WAN Access Type – WiMAX (CBR-971 only)

If you are using WiMAX as the WAN Type, please select **WiMAX** and fill in the required information as follows to directly access Internet via connected WiMAX adapter.

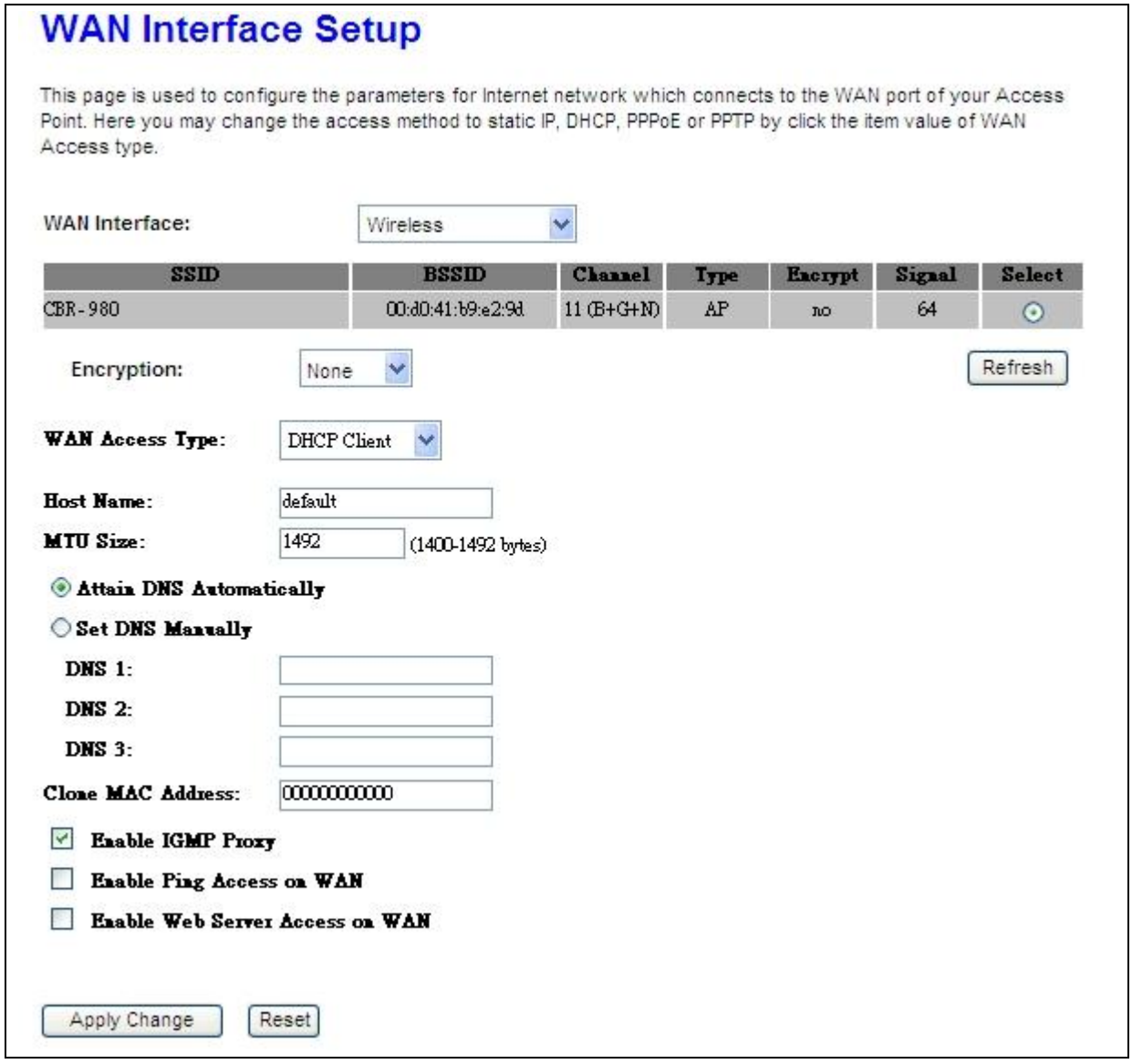

WAN Interface Setup
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.
WAN Interface:
WiMAX
Operator:
Global Mobile
User Name:
username@isp.com
Password:
password
Attain DNS Automatically
Set DNS Manually
DNS 1:
DNS 2:
DNS 3:
Clone MAC Address:
000000000000
Enable IGMP Proxy
Enable Ping Access on WAN
Enable Web Server Access on WAN
Apply Change
Reset

Item	Description
Operator	Select Service Provider. (predefined, contents vary by region).
User Name	Enter your WiMAX user name here.
Password	Enter your password here.
DNS	If ISP provides you DNS information, please select **Attain DNS automatically,** otherwise select **Set DNS Manually** and input the DNS information into the

	blank.
Clone MAC Address	Copy the MAC address from the device you had registered to your ISP if your ISP asks for the specific MAC Address.
Enable IGMP Proxy	The **Internet Group Management Protocol (IGMP)** is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. You can choose to enable **IGMP Proxy** to provide service.
Enable Ping Access on WAN	Select **Enable Ping Access on WAN**, will make WAN IP address response to any ping request from Internet users. It is a common way for hacker to ping public WAN IP address, to see is there any WAN IP address available.
Enable Web Server Access on WAN	This option is to enable **Web Server Access** function on WAN.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

4.1.1.4 WAN Access Type – Wireless

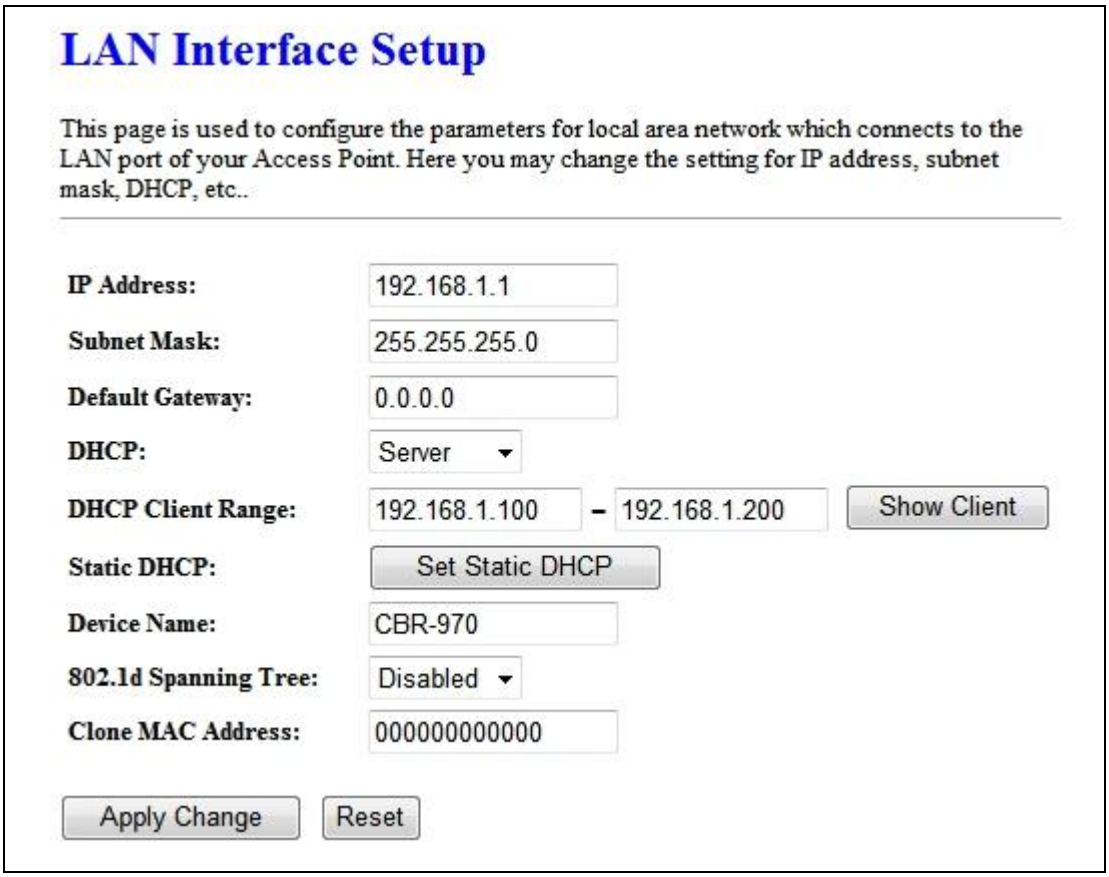
If you are connecting the internet via wireless, please select **Wireless** and its associated settings will show up underneath at the same time.



You can see a list of available Wireless networks. Select you preferred one to connect and the Encryption type form the drop-down list.

4.1.2 LAN Interface Setup

This page is used to configure the parameters for local area network that connects to the LAN ports of your router. Here you may change the setting for IP address, subnet mask, DHCP, etc.



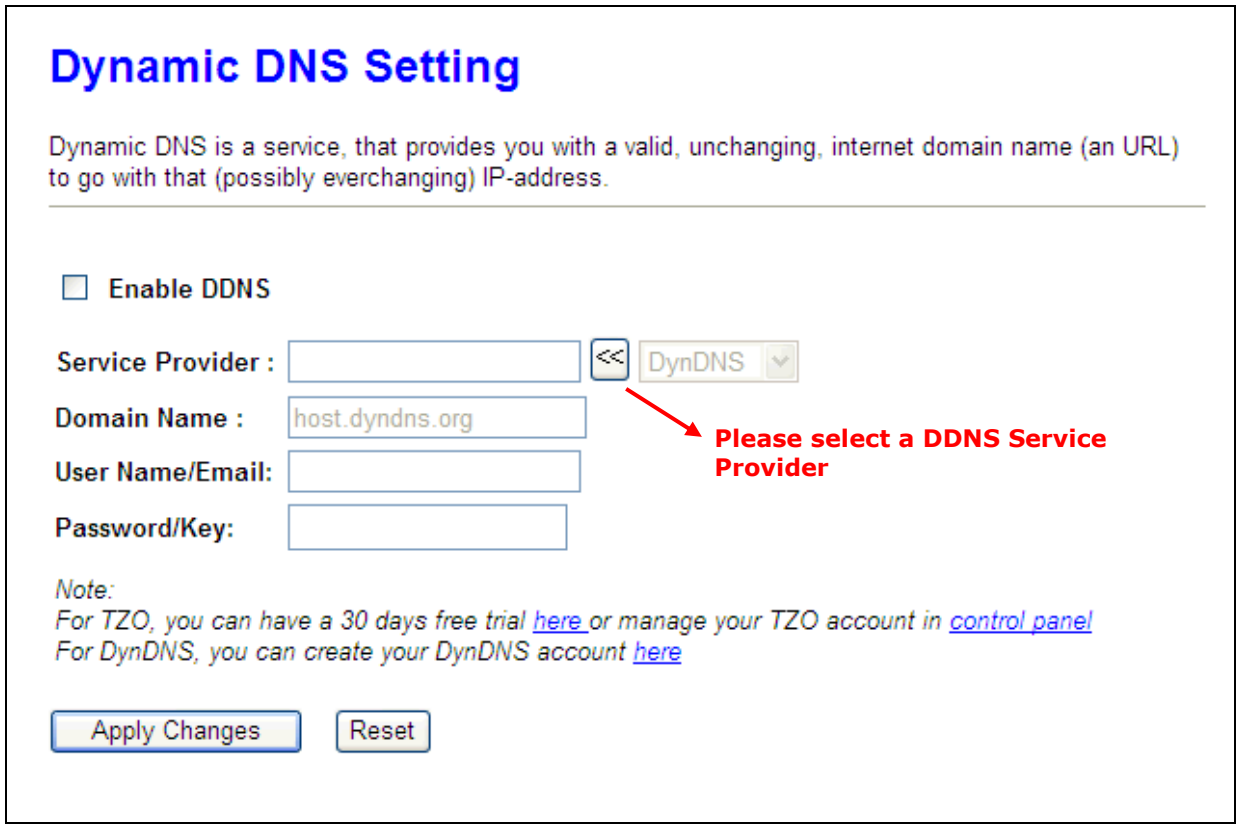
Item	Description
IP Address	The default IP address is **192.168.1.1**
Subnet Mask	Please enter the Subnet Mask address
Default Gateway	Please enter the Default Gateway address for LAN interface.
DHCP	Click to select **Disabled, Client** or **Server** in different operation mode of LAN access point.
DHCP Client Range	Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range
Static DHCP	Configures how static DHCP address are assigned to client (only available when DHCP server is enabled)
Device Name	Configures the device name of the router.
802.1d Spanning Tree	IEEE 802.1d **Spanning Tree Protocol** (**STP**) is a link layer network protocol that ensures a loop-free topology for any bridged LAN. Select enable or disable the IEEE 802.1d Spanning Tree function from

	pull-down menu.
Clone MAC Address	If your ISP asks you to enter a specific MAC Address, please input the correct info at the column.
Apply Change & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

4.1.3 Dynamic DNS Setting

You can assign a fixed host and domain name to a dynamic Internet IP address. Each time the router boots up, it will re-register its domain-name-to-IP-address mapping with the DDNS service provider. This is the way Internet users can access the router through a domain name instead of its IP address.

Note: make sure that you have registered with a DDNS service provider before enabling this feature.


Dynamic DNS Setting
Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.
Enable DDNS
Service Provider :
<<
DynDNS
Domain Name :
host.dyndns.org
User Name/Email:
Password/Key:
Please select a DDNS Service Provider
Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here
Apply Changes
Reset

Please enter **Domain Name**, **User Name/Email**, and **Password/Key**. After entering, click on **Apply Changes** to save the setting, or you may click on **Reset** to clear all the input data.

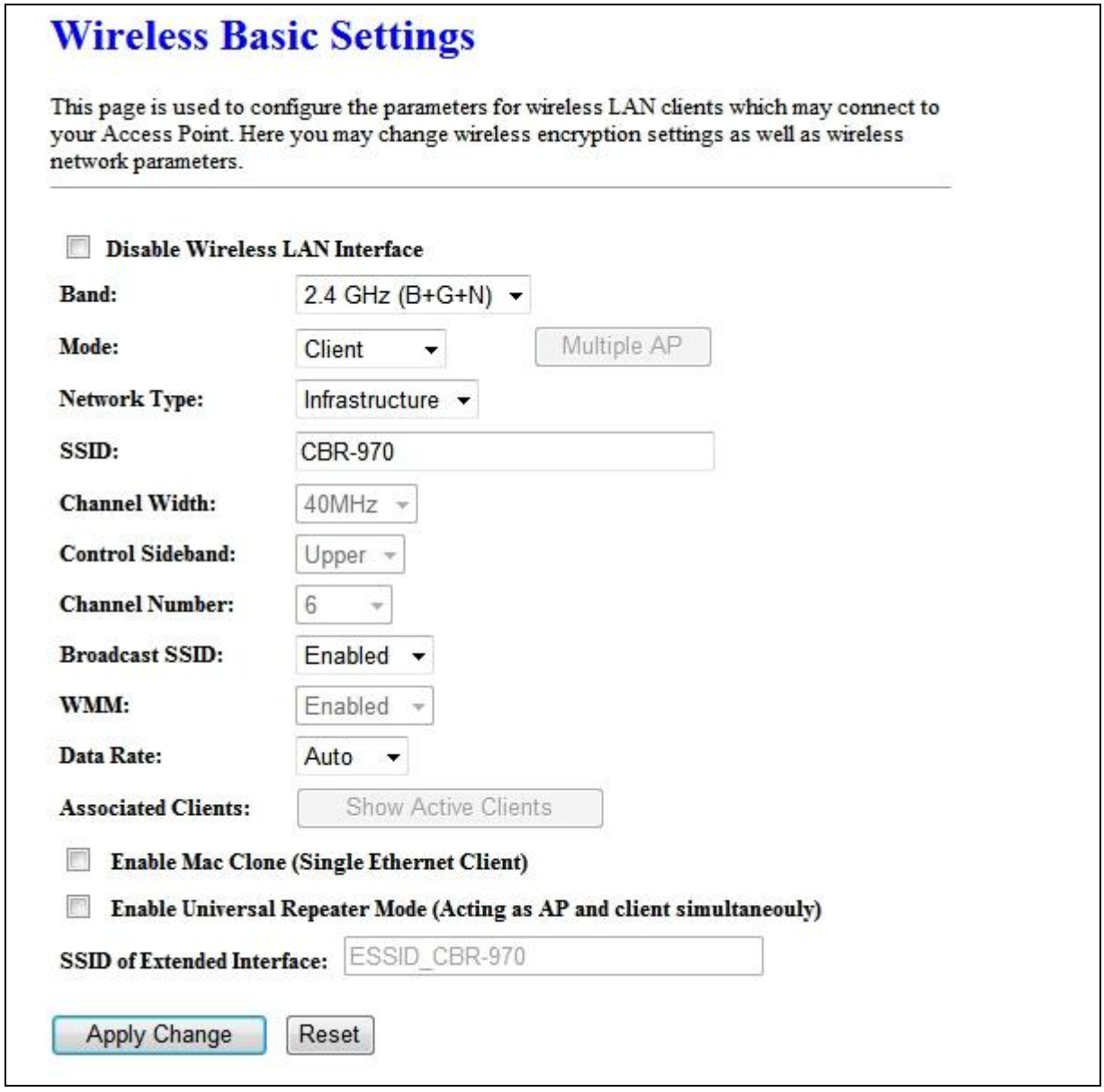
Item	Description
Enable/Disable DDNS	Select enable to use DDNS function. Each time your IP address to WAN is changed, and the information will be updated to DDNS service provider automatically.
Service Provider	Choose correct Service Provider from drop-down list, here including DynDNS, TZO, ChangeIP, Eurodns, OVH, NO-IP, ODS, Regfish embedded in CBR-970/971.
User Name/Email	User name is used as an identity to login Dynamic-DNS service.
Password/Key	Password is applied to login Dynamic-DNS service.
Apply & Cancel	Click on **Apply** button to continue. Click on **Cancel** button to clear the setting on this page.

4.2 Wireless Setup

The category includes **Basic Settings**, **Advanced Settings**, **Security**, **Access Control**, **WDS settings**, and **WPS**. Please read below for the setting instruction.

4.2.1 Wireless Basic Settings

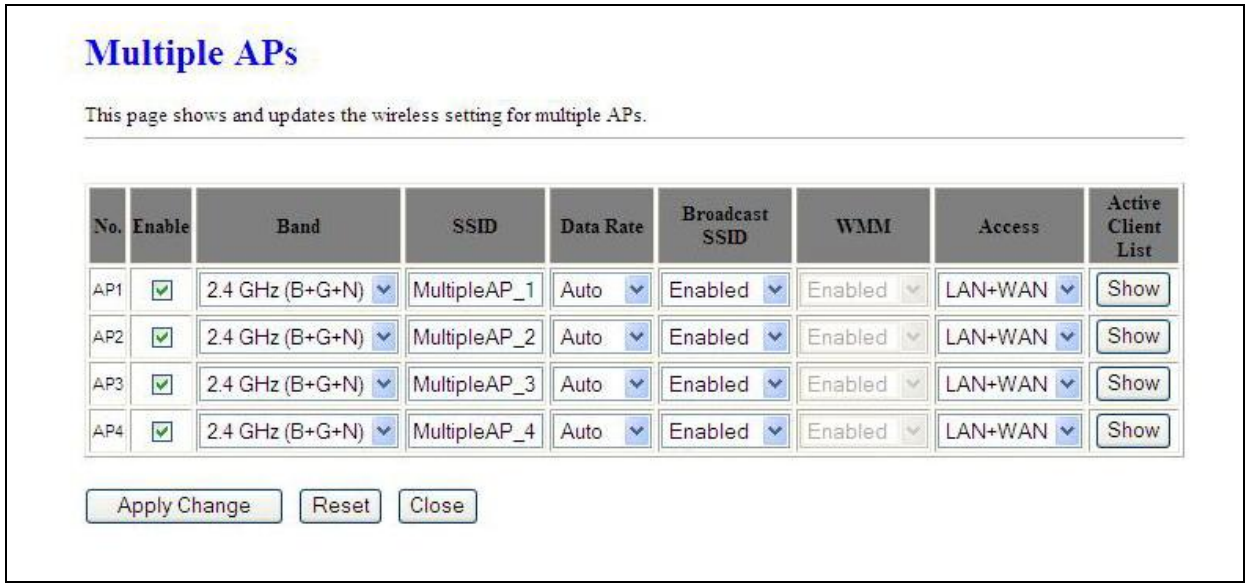
The Wireless Basic Settings include Band, Mode, SSID, Channel Number and other wireless settings.


Wireless Basic Settings
This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.
Disable Wireless LAN Interface
Band:
2.4 GHz (B+G+N)
Mode:
Client
Multiple AP
Network Type:
Infrastructure
SSID:
CBR-970
Channel Width:
40MHz
Control Sideband:
Upper
Channel Number:
6
Broadcast SSID:
Enabled
WMM:
Enabled
Data Rate:
Auto
Associated Clients:
Show Active Clients
Enable Mac Clone (Single Ethernet Client)
Enable Universal Repeater Mode (Acting as AP and client simultaneouly)
SSID of Extended Interface:
ESSID_CBR-970
Apply Change
Reset

Item	Description
Disable Wireless LAN Interface	Turn off the wireless service.
Band	Please select the frequency. It has 6 options: 2.4 GHz (B/G/N/B+G/G+N/B+G+N).
Mode	Please select the mode. It has 3 modes to select:(AP, Client, WDS, AP+WDS). **Multiple APs** provides users another 4 different SSID for connection. Users can add or limit the properties for each connection. Please check Section 4.2.1.1
SSID	Service Set identifier, the default SSID is **CNet**, users can define to any.
Channel Width	Please select the channel width, it has 2 options: 20MHZ, and 40MHZ.
Control Sideband	Enable this function will control your router use lower or upper channel.
Channel Number	Please select the channel; it has Auto, 1, 2~11 or 13 options.
Broadband SSID	User may choose to enable **Broadcast SSID** or not.
Data Rate	Please select the data transmission rate.
Associate Clients	Check the AP connectors and the Wireless connecting status.
Enable MAC Clone (Single Ethernet Client)	Clone the MAC address for ISP to identify.
Enable Universal Repeater Mode (Acting as AP and Client simultaneously)	Allow to equip with the wireless way conjunction upper level, provide the bottom layer user link in wireless and wired way in the meantime. (The IP that bottom layer obtains is from upper level.) Please check Section 4.2.1.2
SSID of Extended Interface	While linking the upper level device in wireless way, you can set SSID to give the bottom layer user search.
Apply Change & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

4.2.1.1 Multiple APs

Multiple APs provides users another 4 different SSIDs for connection. Each SSID could be set with different data rate, WMM and access type.

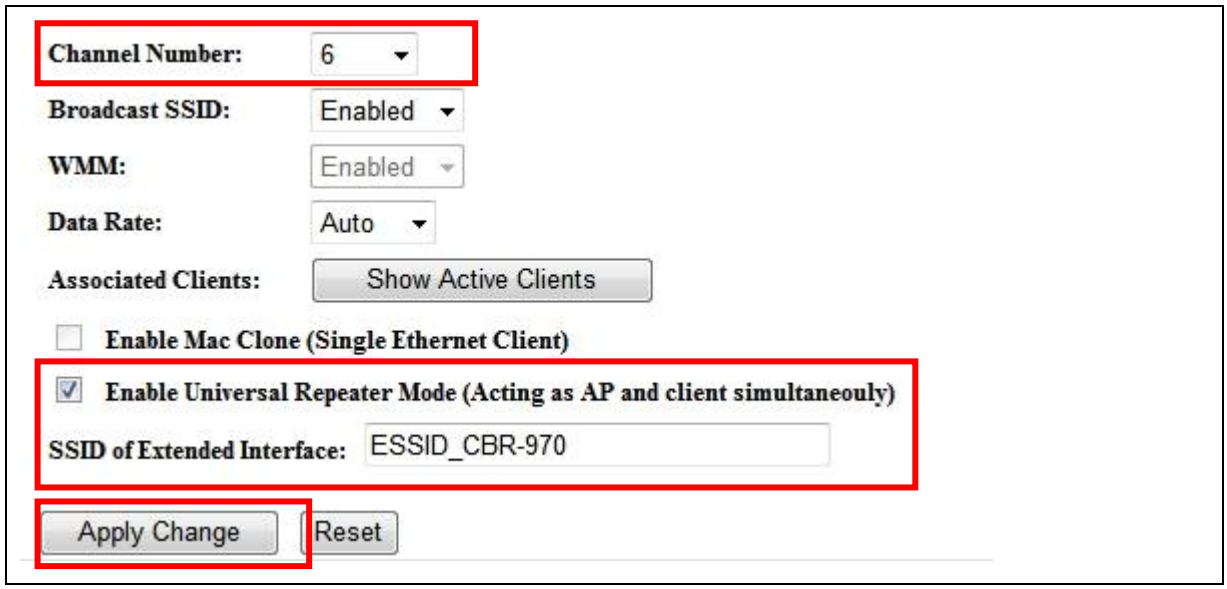

Multiple APs
This page shows and updates the wireless setting for multiple APs.
No. Enable Band SSID Data Rate Broadcast SSID WMM Access Active Client List
AP1 2.4 GHz (B+G+N) MultipleAP_1 Auto Enabled Enabled LAN+WAN Show
AP2 2.4 GHz (B+G+N) MultipleAP_2 Auto Enabled Enabled LAN+WAN Show
AP3 2.4 GHz (B+G+N) MultipleAP_3 Auto Enabled Enabled LAN+WAN Show
AP4 2.4 GHz (B+G+N) MultipleAP_4 Auto Enabled Enabled LAN+WAN Show
Apply Change
Reset
Close

Item	Description
Enable	Enable or disable the service.
Band	Select the frequency.
SSID	Enter the SSID.
Data Rate	Select the data transmission rate.
Access	Enable this function can let clients use two access types: a. LAN+WAN: the client can access to the Internet and access in the router's GUI. b. WAN: the client can only access to the Internet.
Active Client List	Display the properties of the client which is connecting successfully.
Apply Changes	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

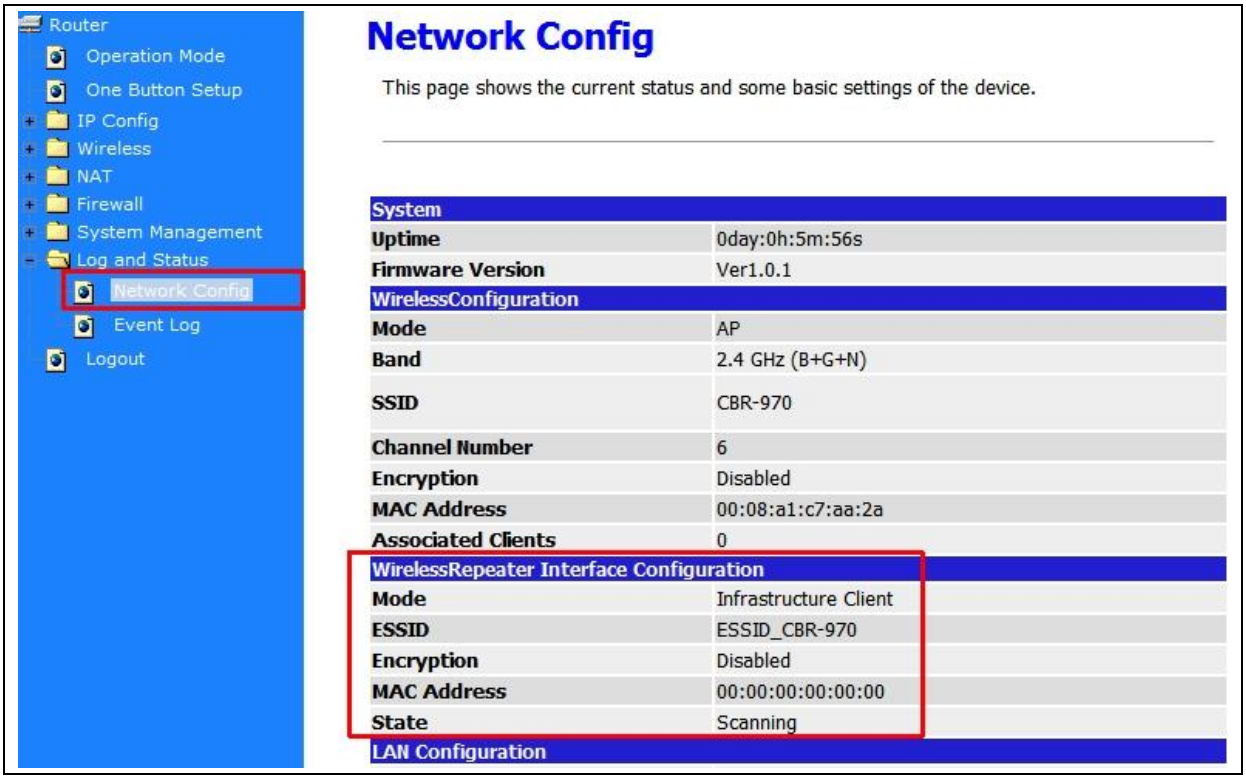
4.2.1.2 Enable Universal Repeater Mode (Acting as AP Client simultaneously)

The router can act as Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to service all wireless stations within its coverage.

Example: When users enable the Universal Repeater to connect to the upper level device, please fill in the upper level device's channel and SSID. Click on **Apply Changes** to save the settings. (Please disable the DHCP service first)

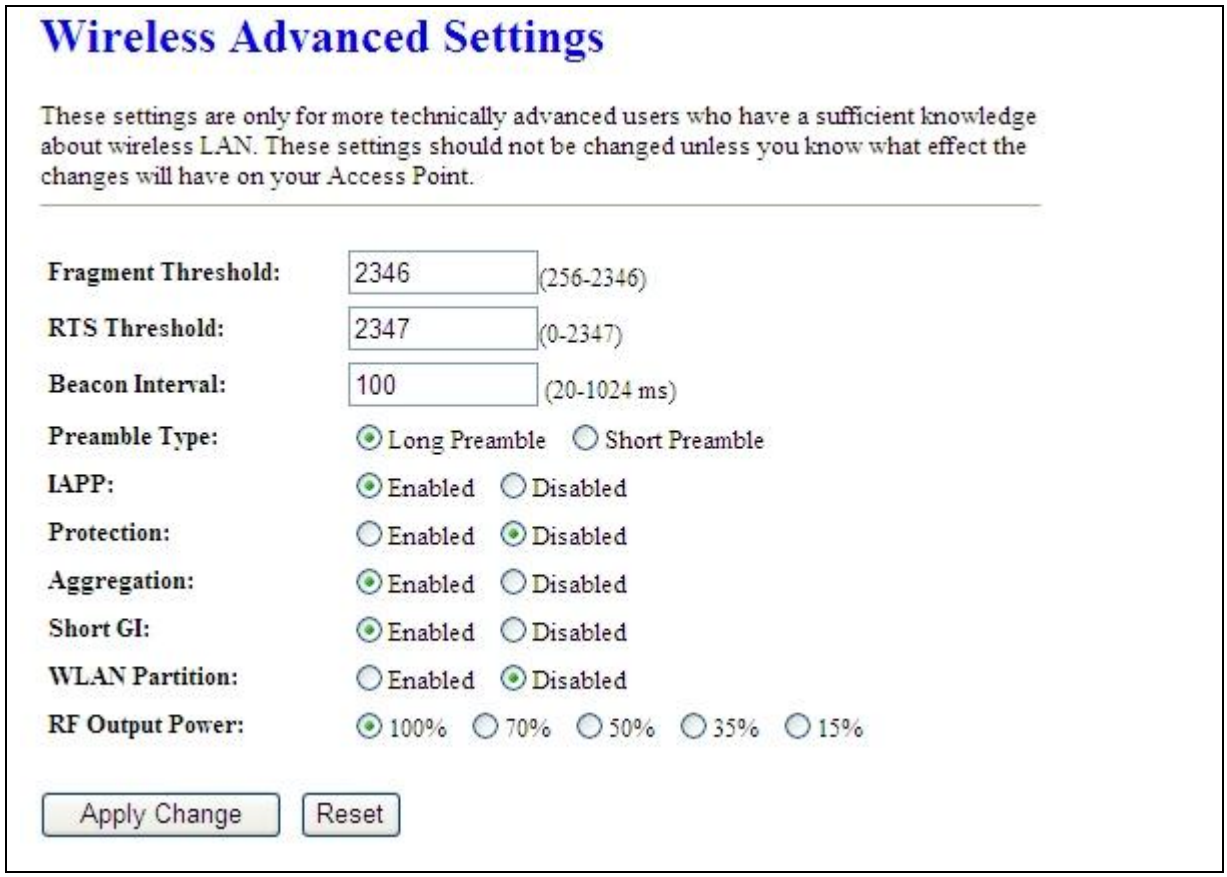


Users can use the Network Configuration page to check the information about "**Wireless Repeater Interface Configuration**".


Router
Operation Mode
One Button Setup
IP Config
Wireless
NAT
Firewall
System Management
Log and Status
Network Config
Event Log
Logout
Network Config
This page shows the current status and some basic settings of the device.
System
Uptime 0day:0h:5m:56s
Firmware Version Ver1.0.1
WirelessConfiguration
Mode AP
Band 2.4 GHz (B+G+N)
SSID CBR-970
Channel Number 6
Encryption Disabled
MAC Address 00:08:a1:c7:aa:2a
Associated Clients 0
WirelessRepeater Interface Configuration
Mode Infrastructure Client
ESSID ESSID_CBR-970
Encryption Disabled
MAC Address 00:00:00:00:00:00
State Scanning
LAN Configuration

4.2.2 Wireless Advanced Settings

In Advanced Settings page, more 802.11 related parameters are tunable


Wireless Advanced Settings
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.
Fragment Threshold: 2346 (256-2346)
RTS Threshold: 2347 (0-2347)
Beacon Interval: 100 (20-1024 ms)
Preamble Type: Long Preamble Short Preamble
IAPP: Enabled Disabled
Protection: Enabled Disabled
Aggregation: Enabled Disabled
Short GI: Enabled Disabled
WLAN Partition: Enabled Disabled
RF Output Power: 100% 70% 50% 35% 15%
Apply Change
Reset

Item	Description
Fragment Threshold	To identify the maxima length of packet, the over length packet will be fragmentized. The allowed range is 256-2346, and default length is 2346
RTS Threshold	This value should remain at its default setting of 2347. The range is 0~2347. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the present RTS threshold size, the RTS/CTS mechanism will not be enabled. The router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. Fill the range from 0 to 2347 into this blank.
Beacon Interval	Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. The allowed setting range is 20-1024 ms.
Preamble Type	PLCP is Physical layer convergence protocol and PPDU is PLCP protocol

	data unit during transmission, the PSDU shall be appended to a PLCP preamble and header to create the PPDU. It has 2 options: Long Preamble and Short Preamble.
IAPP	Inter-Access Point Protocol is a recommendation that describes an optional extension to IEEE 802.11 that provides wireless access-point communications among multivendor systems.
Protection	Please select to enable wireless protection or not.
Aggregation	Enable this function will combine several packets to one and transmit it. It can reduce the problem when mass packets are transmitting.
Short GI	Users can get better wireless transmission efficiency when they enable this function.
RF Output Power	Users can adjust RF output power to get the best wireless network environment. Users can choose from 100%, 70%, 50%, 35%, and 15%.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

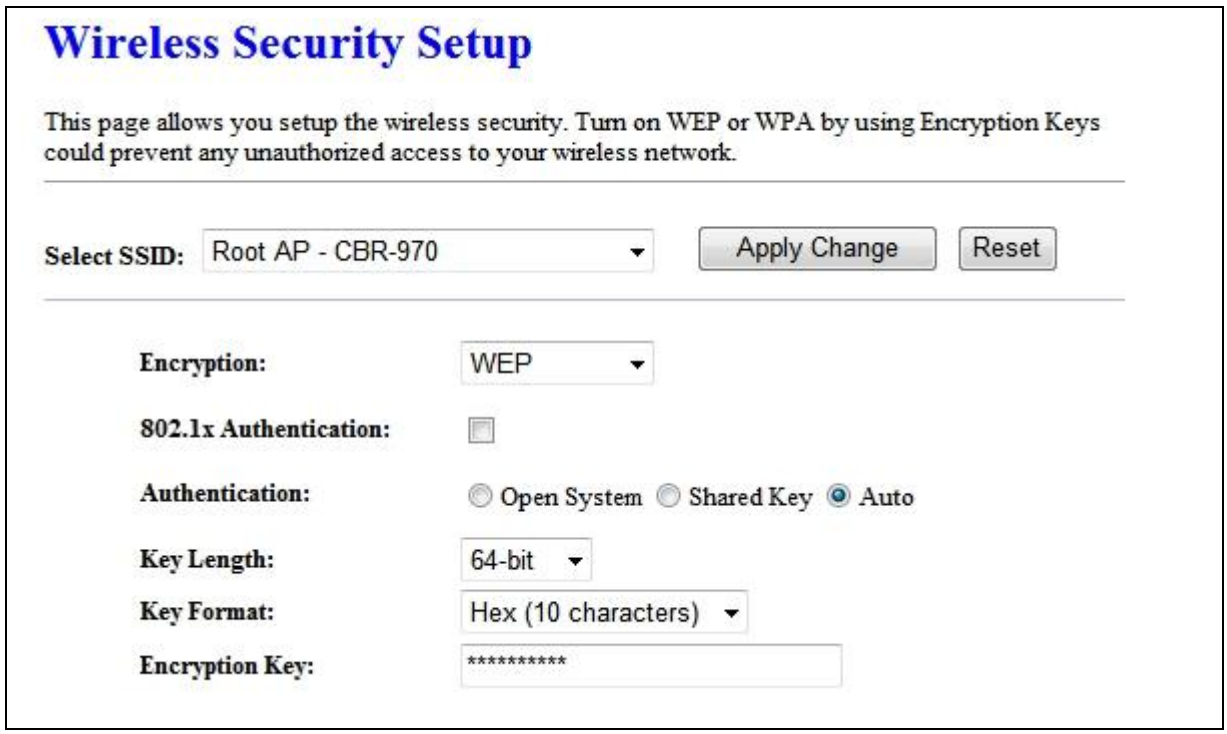
4.2.3 Wireless Security Setup

Here users define the security type and level of the wireless network. Selecting different methods provides different levels of security. **Please note that using any encryption may cause a significant degradation of data throughput on the wireless link**. There are five Encryption types supported: “None”, “WEP”, “WPA (TKIP)”, ”WPA2(AES)”, and “WPA2 Mixed”.

Wireless Security Setup
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.
Select SSID:
Root AP - CBR-970
Apply Change
Reset
Encryption:
Disable
802.1x Authentication:

1. Encryption -- WEP Key

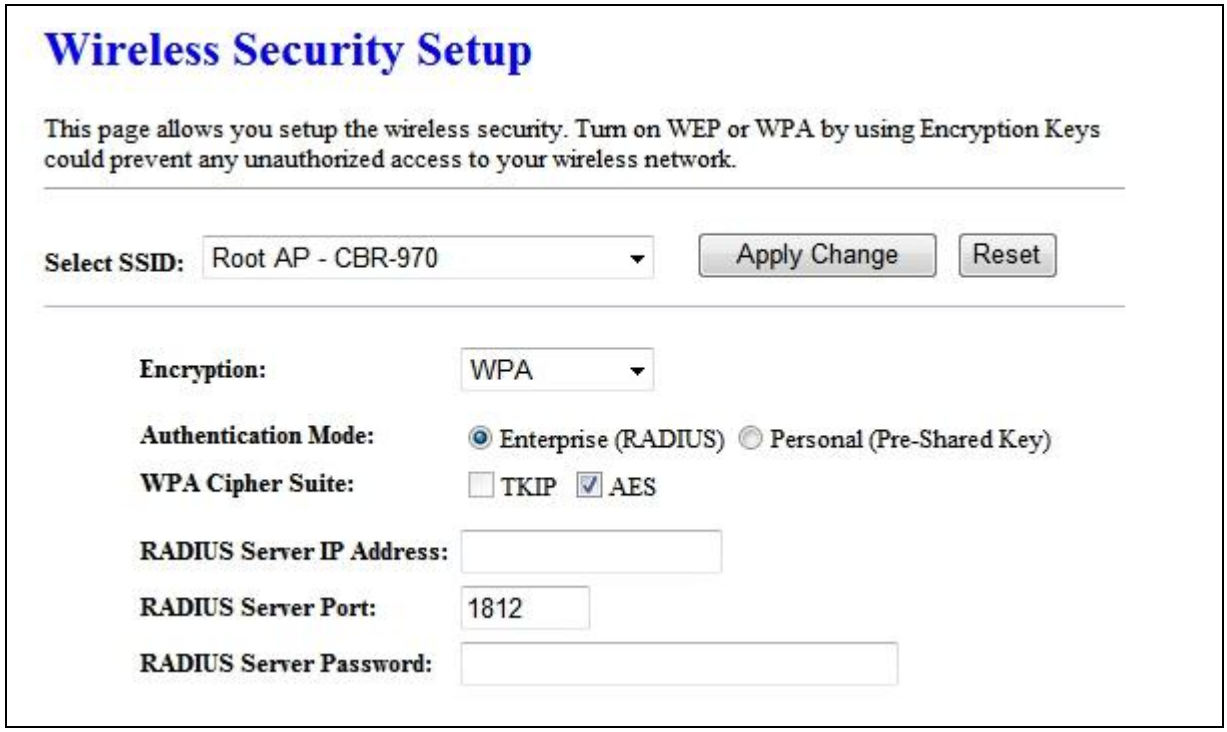
1.1 Set WEP Key: This section provides 64bit and 128bit WEP encryptions and two different shared key formats (ASCII and Hex) for wireless network.



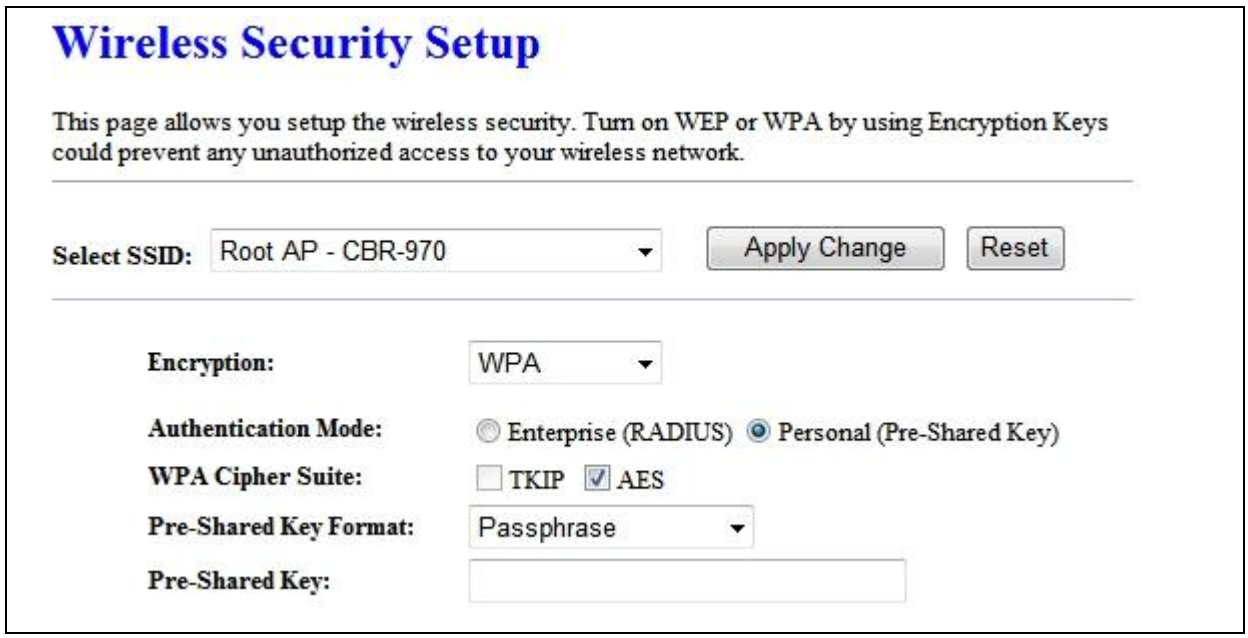
802.1x Authentication: It is a safety system by using authentication to protect your wireless network.

2. Encryption – WPA (WPA, WPA2, and WPA2 Mixed), WPA Authentication Mode

- Enterprise (RADIUS): Please fill in the RADIUS server Port, IP Address, and Password


Wireless Security Setup
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.
Select SSID: Root AP - CBR-970
Apply Change
Reset
Encryption: WPA
Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)
WPA Cipher Suite: TKIP AES
RADIUS Server IP Address:
RADIUS Server Port: 1812
RADIUS Server Password:

- Personal (Pre-Shared Key): Pre-Shared Key type is ASCII Code; the length is between 8 to 63 characters. If the key type is Hex, the key length is 64 characters

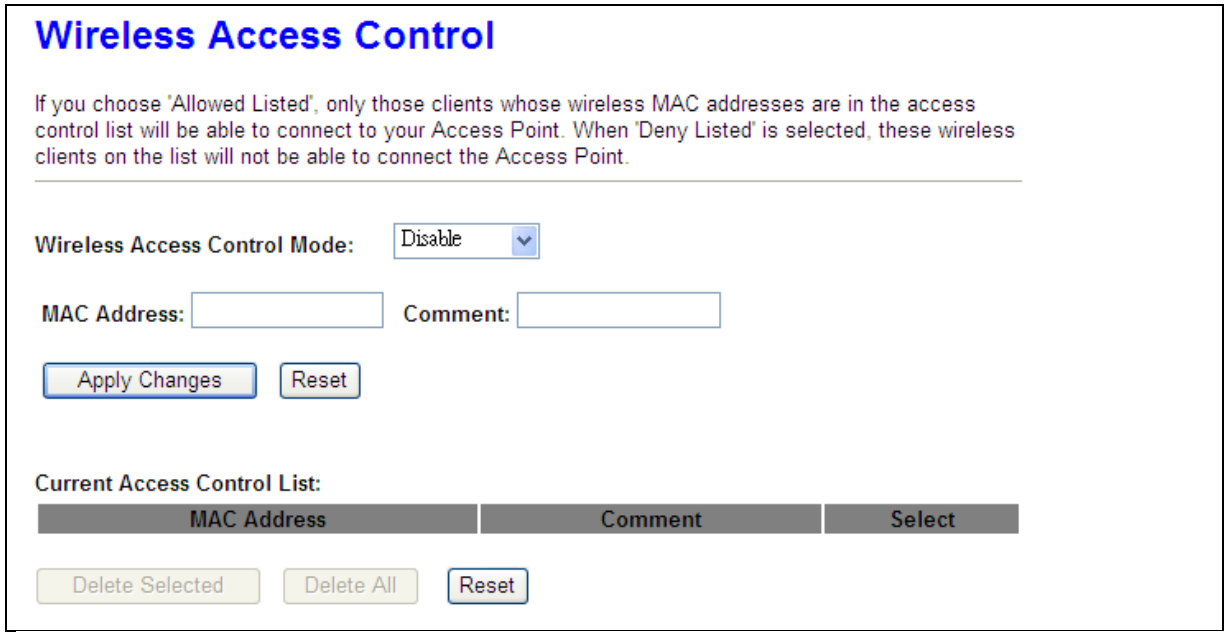

Wireless Security Setup
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.
Select SSID: Root AP - CBR-970
Apply Change
Reset
Encryption: WPA
Authentication Mode: Enterprise (RADIUS) Personal (Pre-Shared Key)
WPA Cipher Suite: TKIP AES
Pre-Shared Key Format: Passphrase
Pre-Shared Key:

3. Apply Change & Reset: Click on **'Apply Changes'** to save setting data. Or click **'Reset'** to reset all

the input data.

4.2.4 Wireless Access Control

Access Control allows user to block or allow wireless clients to access this router. Users can select the access control mode, then add a new MAC address with a simple comment and click on “Apply Changes” to save the new addition. To delete a MAC address, select its corresponding checkbox under the **Select** column and click on “Delete Selected” button.

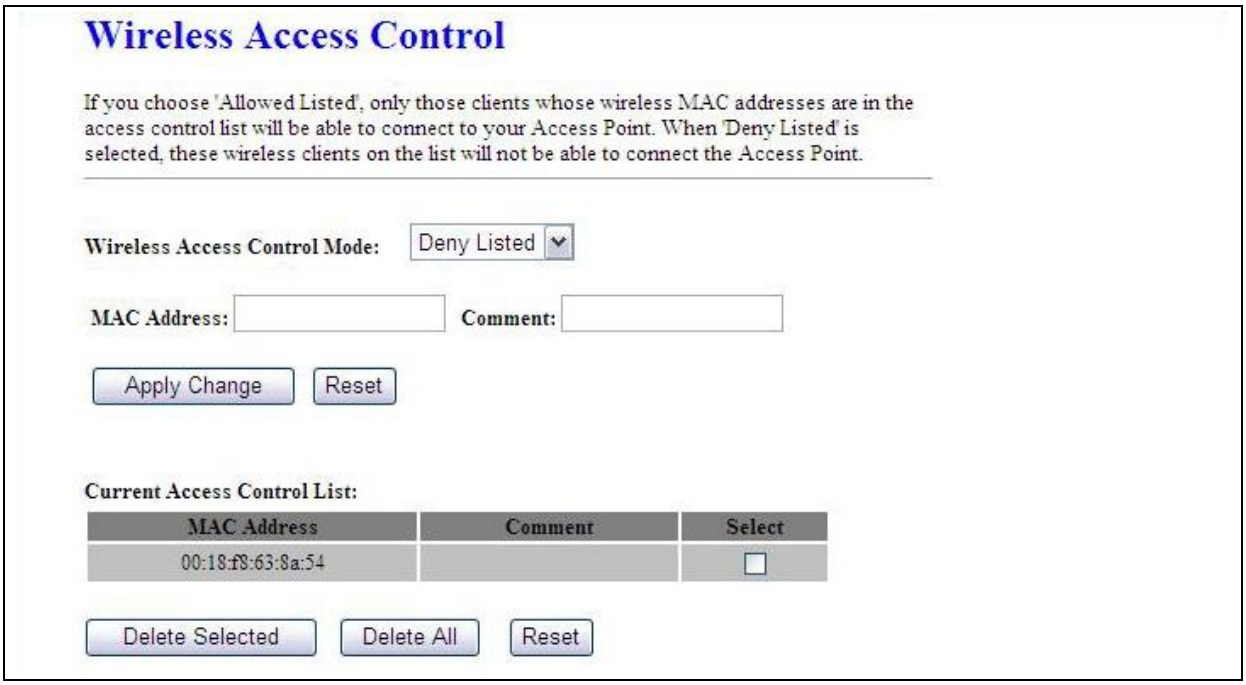

Wireless Access Control
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.
Wireless Access Control Mode:
Disable
MAC Address:
Comment:
Apply Changes
Reset
Current Access Control List:
MAC Address
Comment
Select
Delete Selected
Delete All
Reset

Take the wireless card as the example.

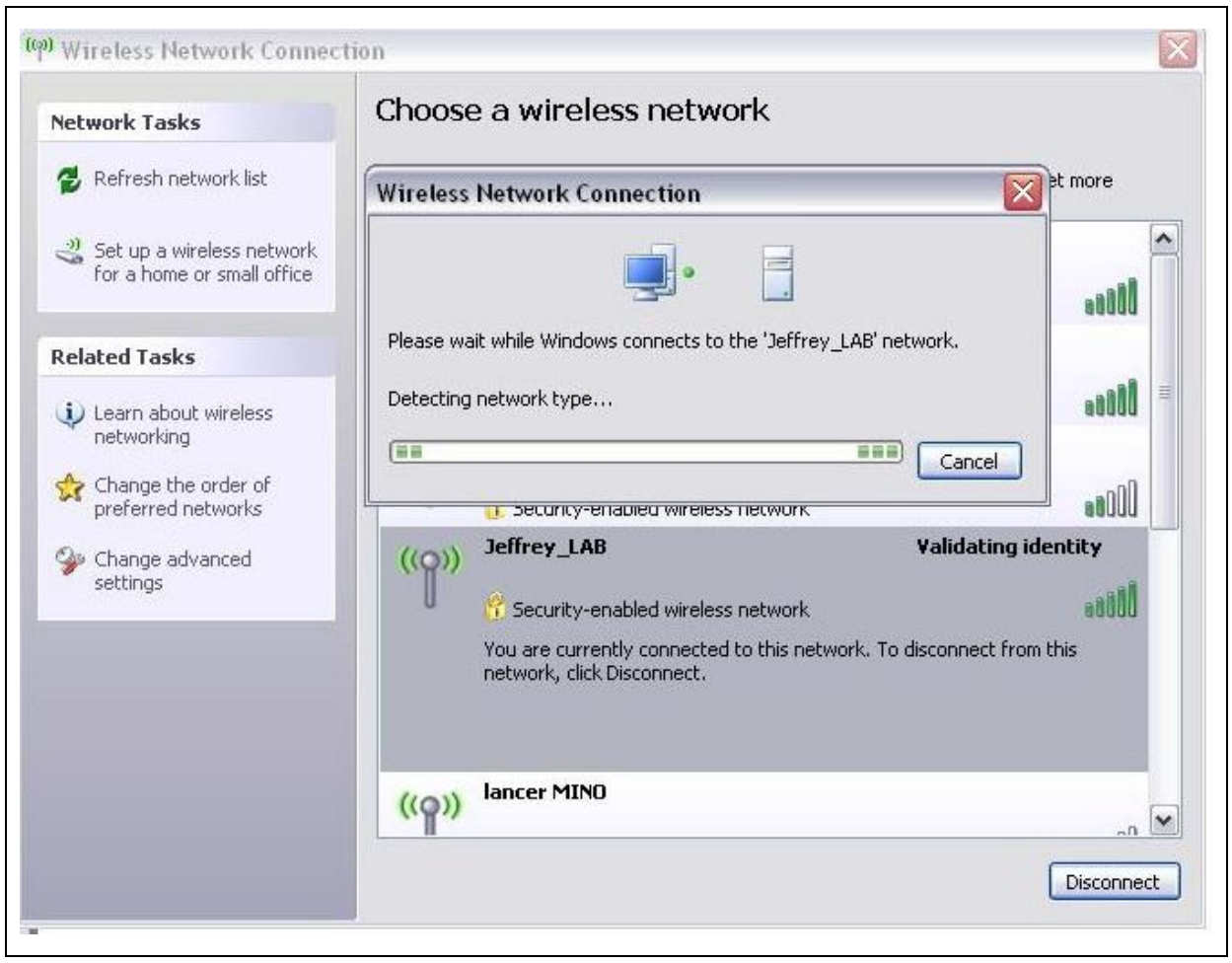
(1) Here is the example. Please select **Deny Listed** in **Wireless Access Control Mode** first, and then fill in the MAC address what you plan to block in the MAC Address field. Click **Apply Changes** to save the setting.

Wireless Access Control
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.
Wireless Access Control Mode:
Deny Listed
MAC Address:
0018F8638A54
Comment:
Apply Change
Reset
Current Access Control List:
MAC Address
Comment
Select
Delete Selected
Delete All
Reset

(2) The MAC address what you set will be displayed on the **Current Access Control List**.

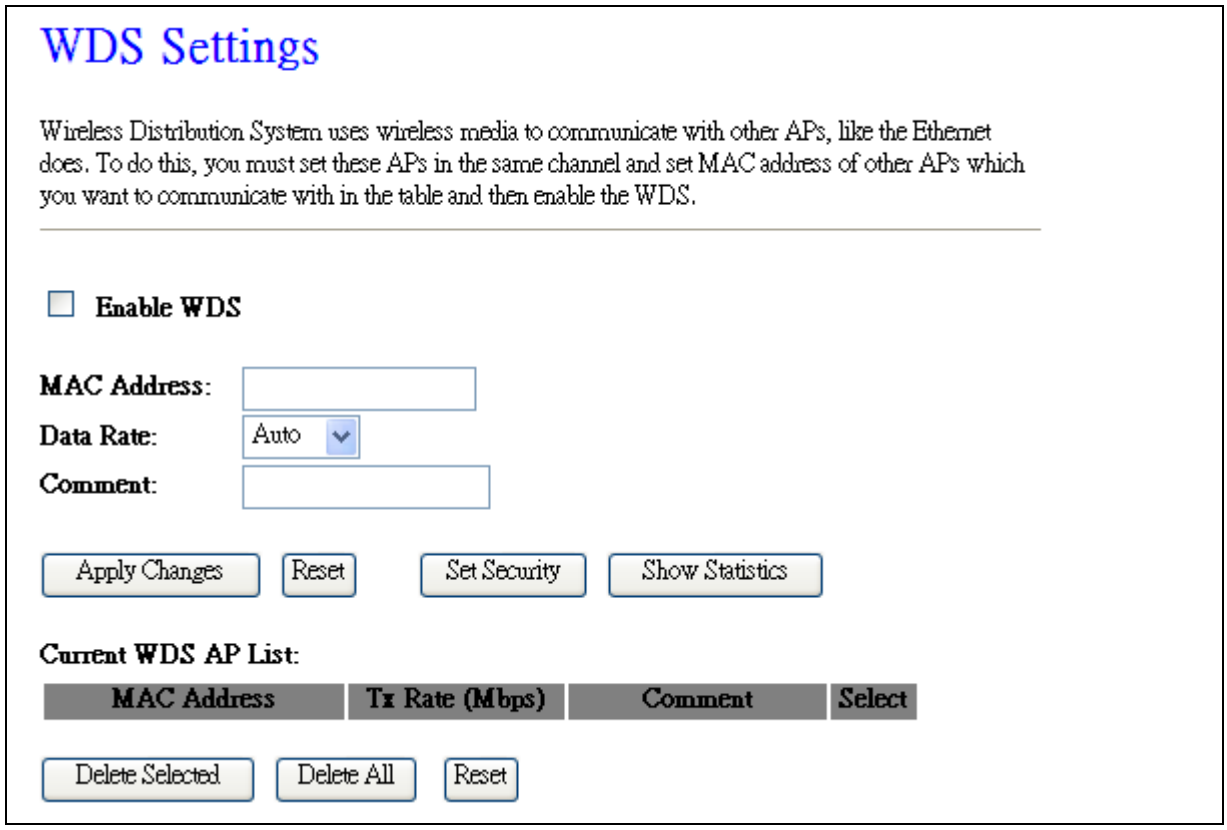

Wireless Access Control
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.
Wireless Access Control Mode:
Deny Listed
MAC Address:
Comment:
Apply Change
Reset
Current Access Control List:
MAC Address
Comment
Select
00:18:f8:63:8a:54
Delete Selected
Delete All
Reset

(3) The wireless client will be denied by the wireless router.

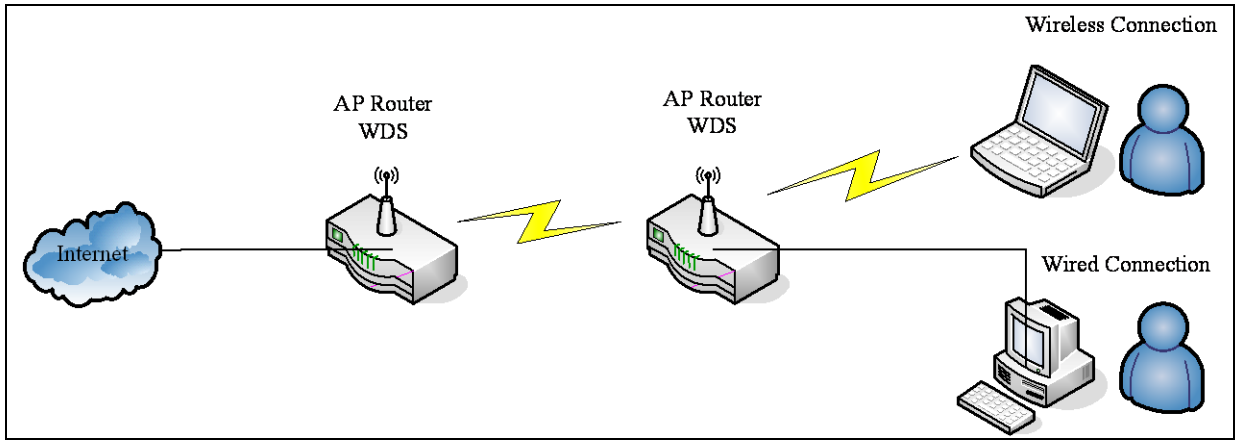

Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
et more
Wireless Network Connection
Please wait while Windows connects to the 'Jeffrey_LAB' network.
Detecting network type...
Cancel
Jeffrey_LAB
Validating identity
Security-enabled wireless network
You are currently connected to this network. To disconnect from this network, click Disconnect.
lancer MINO
Disconnect

4.2.5 WDS Settings

When selected in the Basic Settings page and enabled here, Wireless Distribution System (WDS) enables the router to be used as a wireless bridge. Two Wireless-G Routers in bridge mode can communicate with each other through their wireless interfaces. To accomplish this, all wireless routers should be set to the same channel and the MAC address of other AP / Routers should be entered in the table.

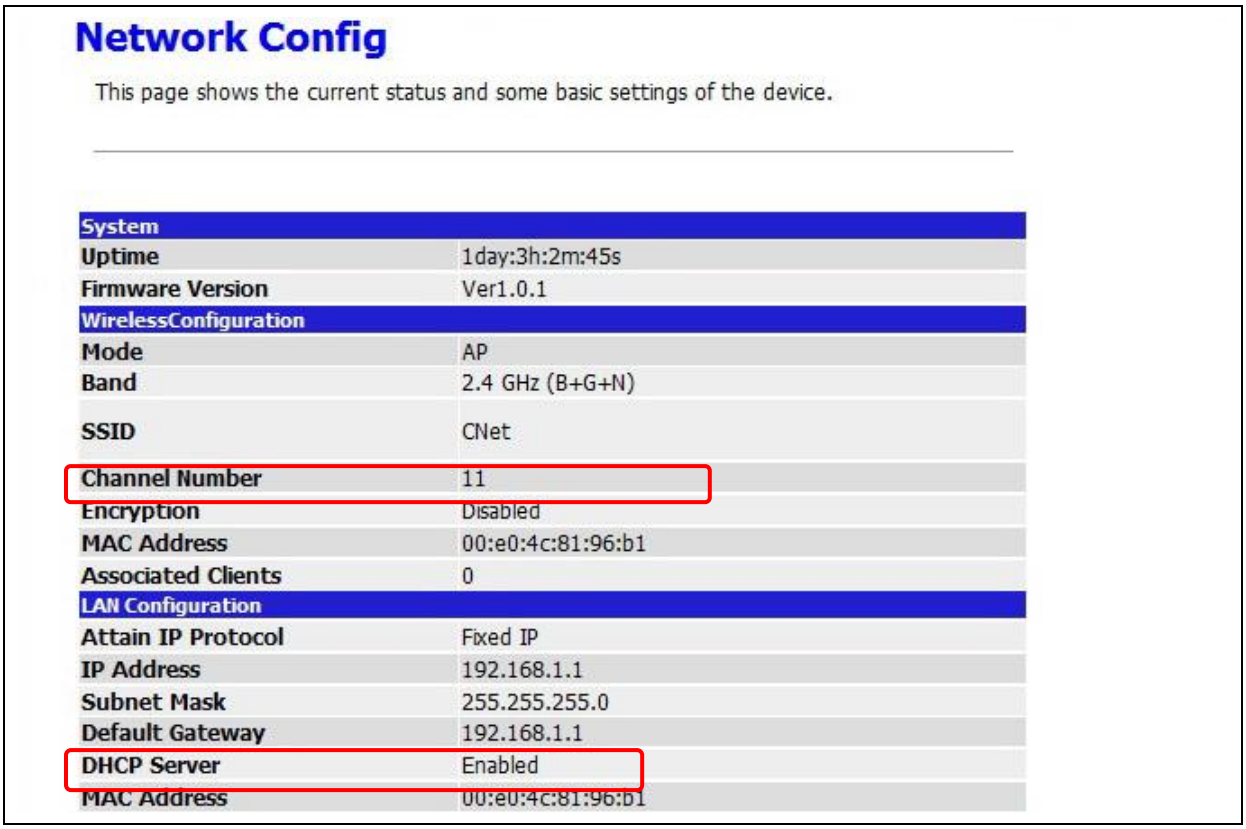

WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.
Enable WDS
MAC Address:
Data Rate:
Auto
Comment:
Apply Changes
Reset
Set Security
Show Statistics
Current WDS AP List:
MAC Address
Tx Rate (Mbps)
Comment
Select
Delete Selected
Delete All
Reset

The WDS explanation as the following picture.



*Please follow the below instructions to setup the WDS connection.

(1) Please check the MAC address and Channel number from the upper lever device.

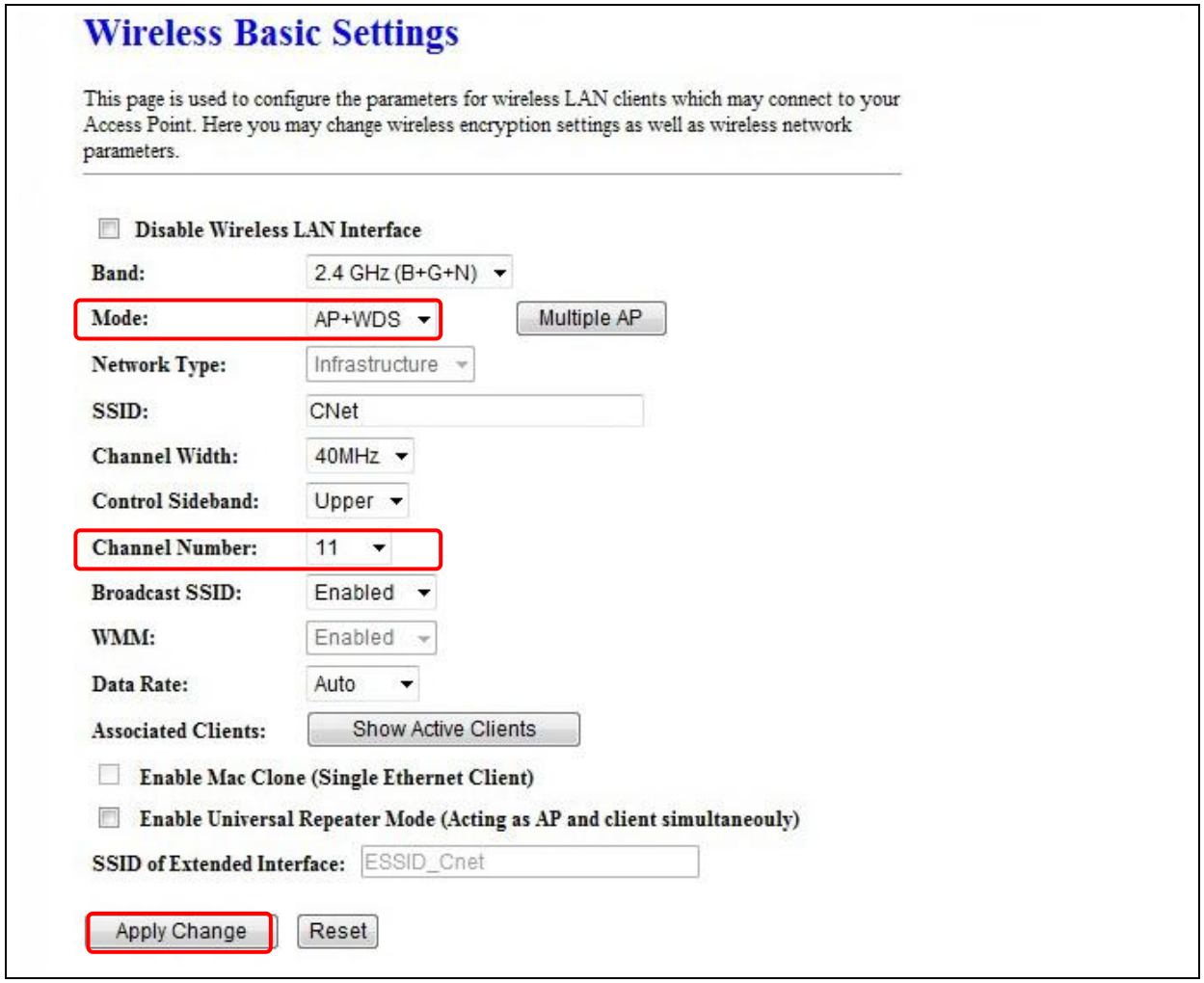


Network Config

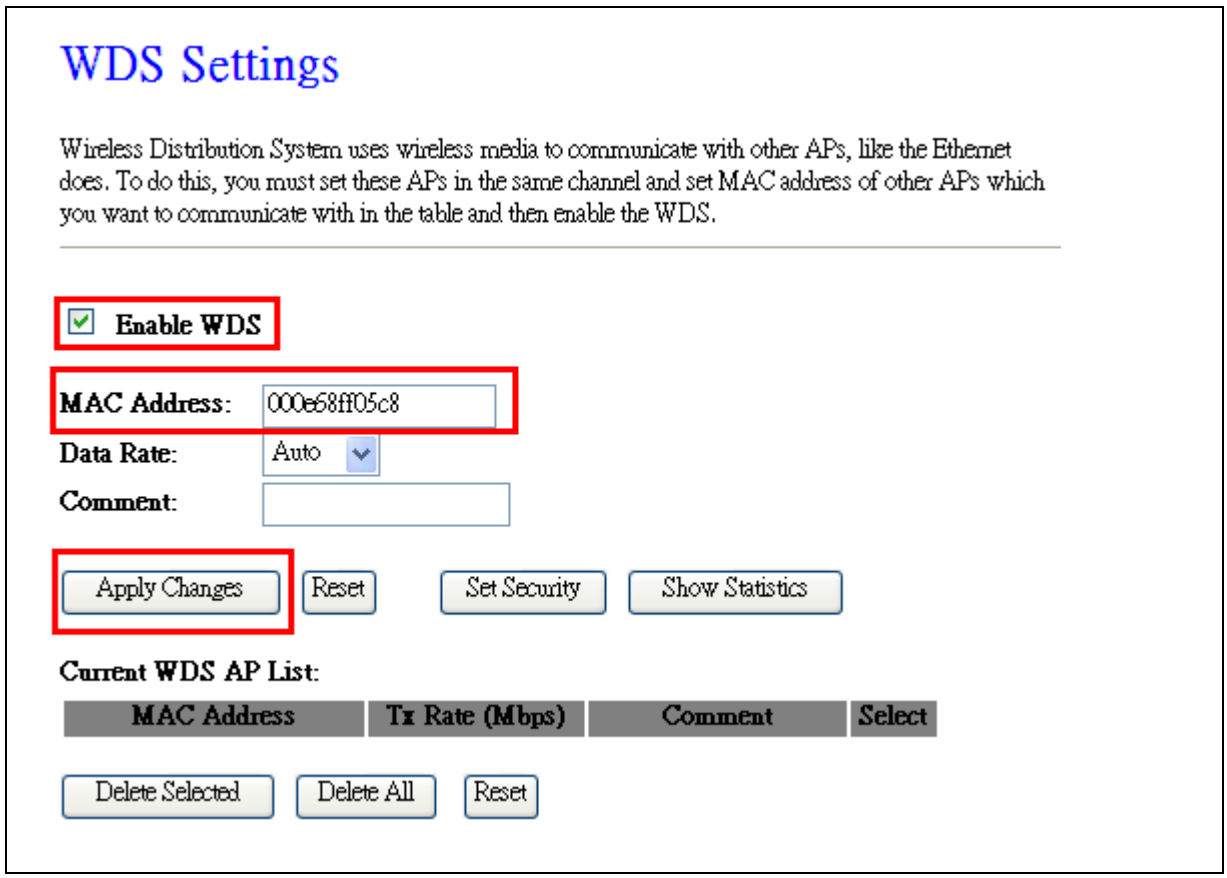
This page shows the current status and some basic settings of the device.

System	
Uptime	1day:3h:2m:45s
Firmware Version	Ver1.0.1
WirelessConfiguration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	CNet
Channel Number	11
Encryption	Disabled
MAC Address	00:e0:4c:81:96:b1
Associated Clients	0
LAN Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DHCP Server	Enabled
MAC Address	00:e0:4c:81:96:b1

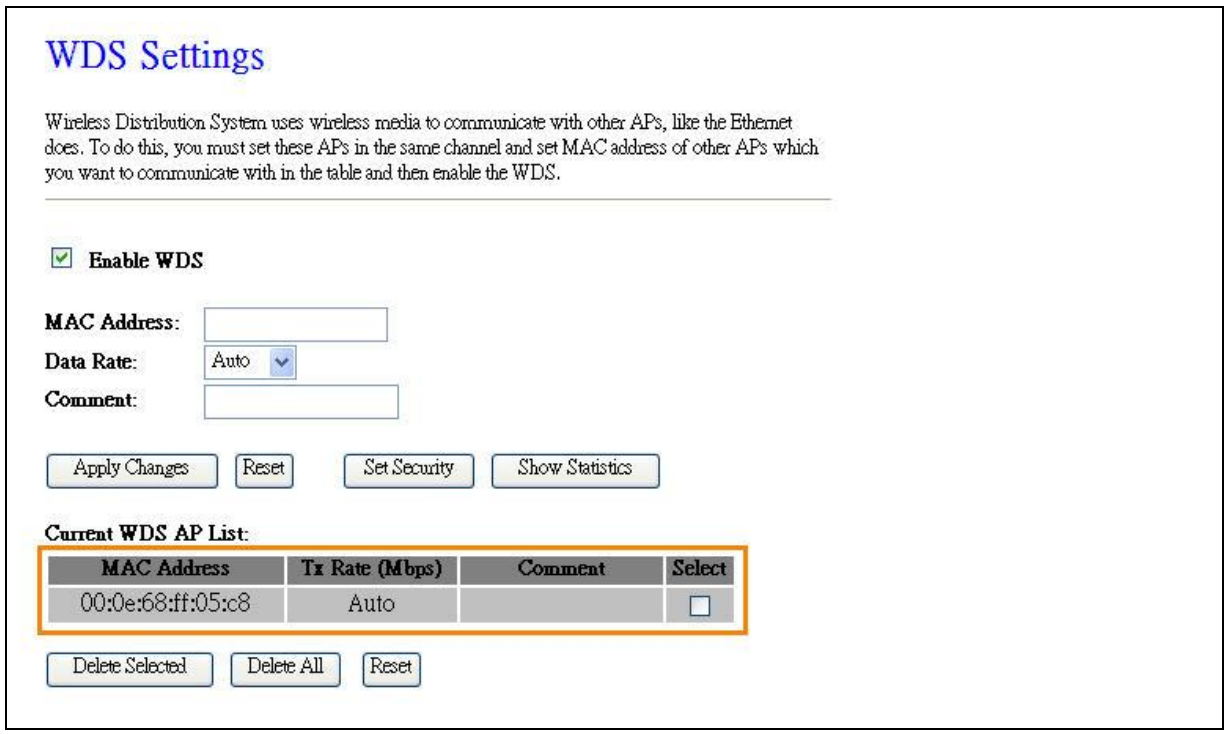
(2) Set the connection mode to “AP+WDS” from “Wireless Basic Setting”, and then select the channel number(in this example is “11”). Click **Apply Changes** to save the setting.



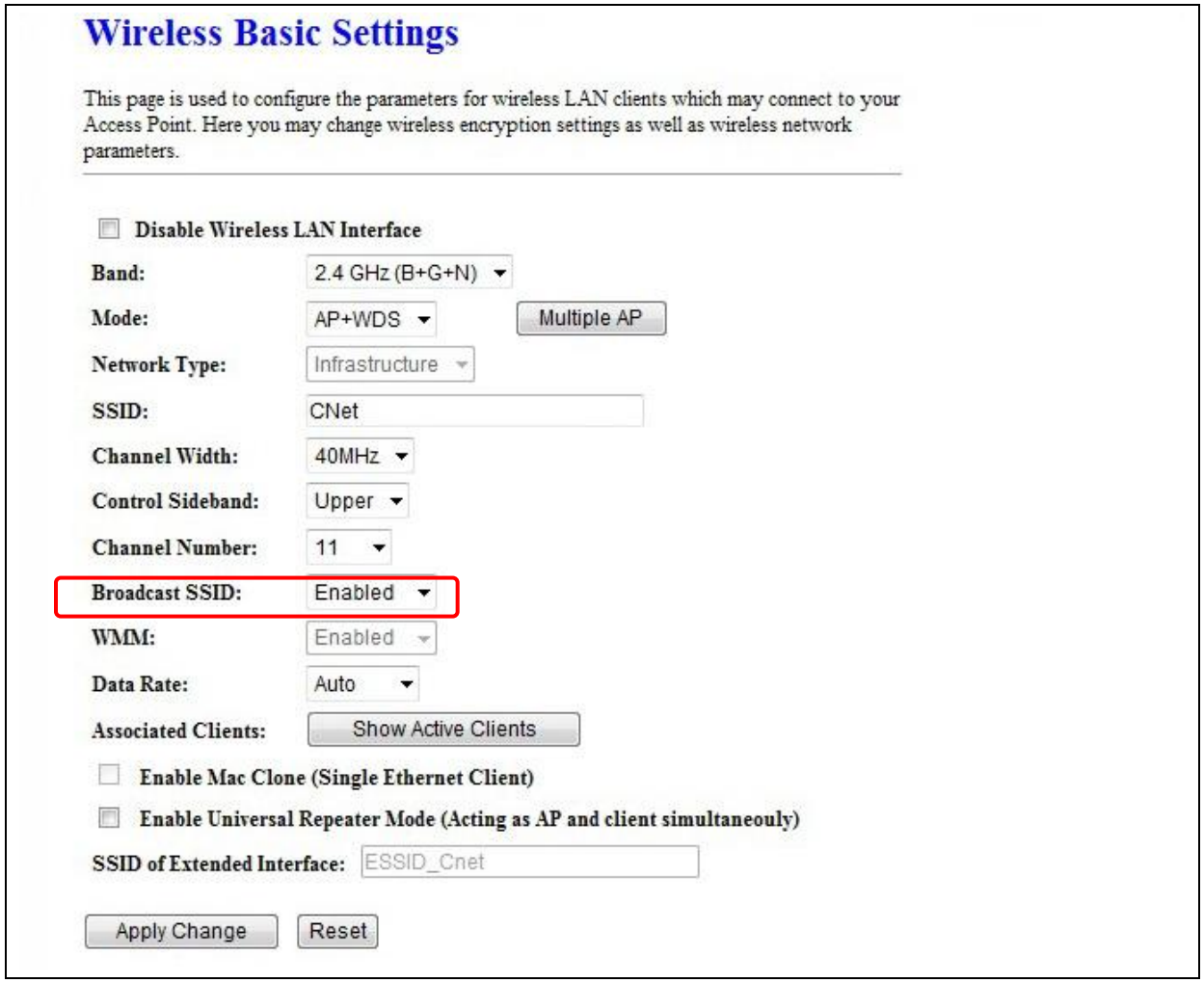
(3) Enable WDS function from the page – “WDS Setting”, and then fill in the upper level device MAC address. Click **Apply Changes** to save the setting data.


WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.
Enable WDS
MAC Address: 000e68ff05c8
Data Rate: Auto
Comment:
Apply Changes
Reset
Set Security
Show Statistics
Current WDS AP List:
MAC Address
Tx Rate (Mbps)
Comment
Select
Delete Selected
Delete All
Reset

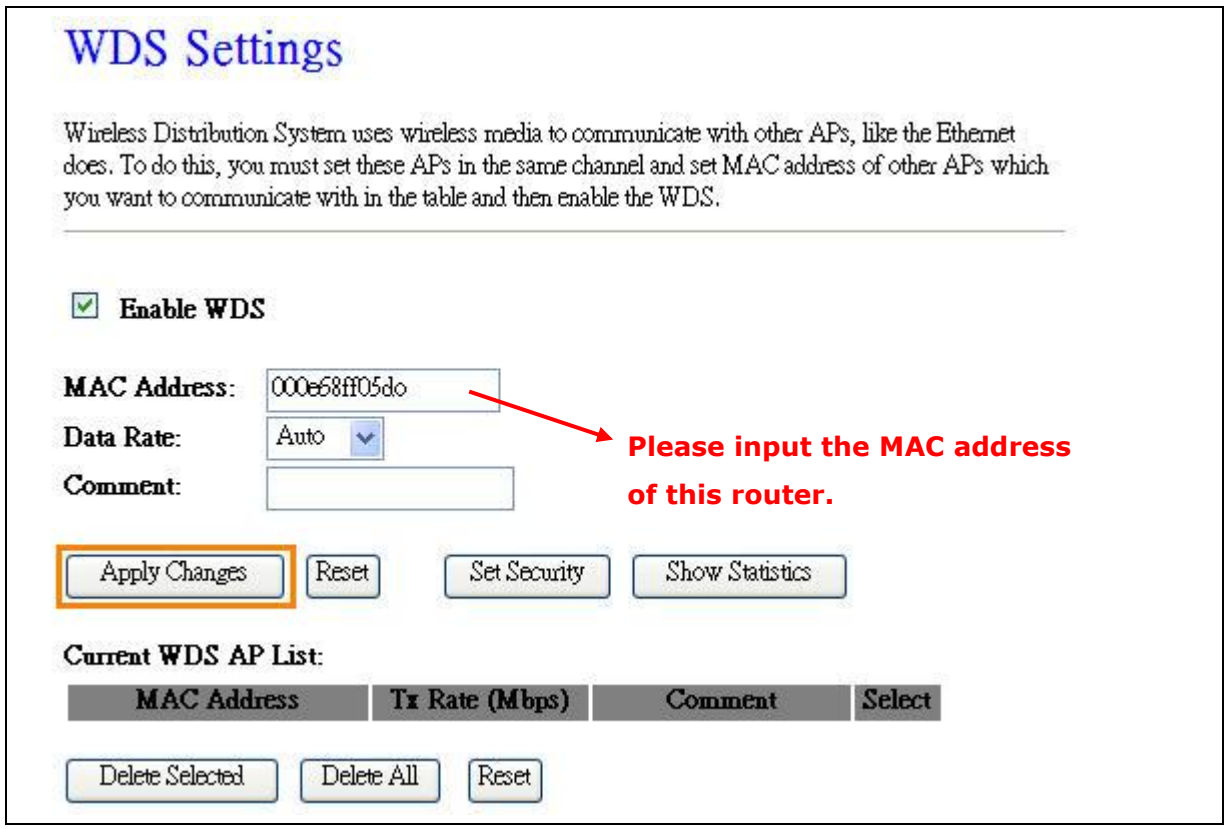
(4) The WDS AP List will show the WDS device MAC address after reboot.


WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.
Enable WDS
MAC Address:
Data Rate: Auto
Comment:
Apply Changes
Reset
Set Security
Show Statistics
Current WDS AP List:
MAC Address
Tx Rate (Mbps)
Comment
Select
00:0e:68:ff:05:c8
Auto
Delete Selected
Delete All
Reset

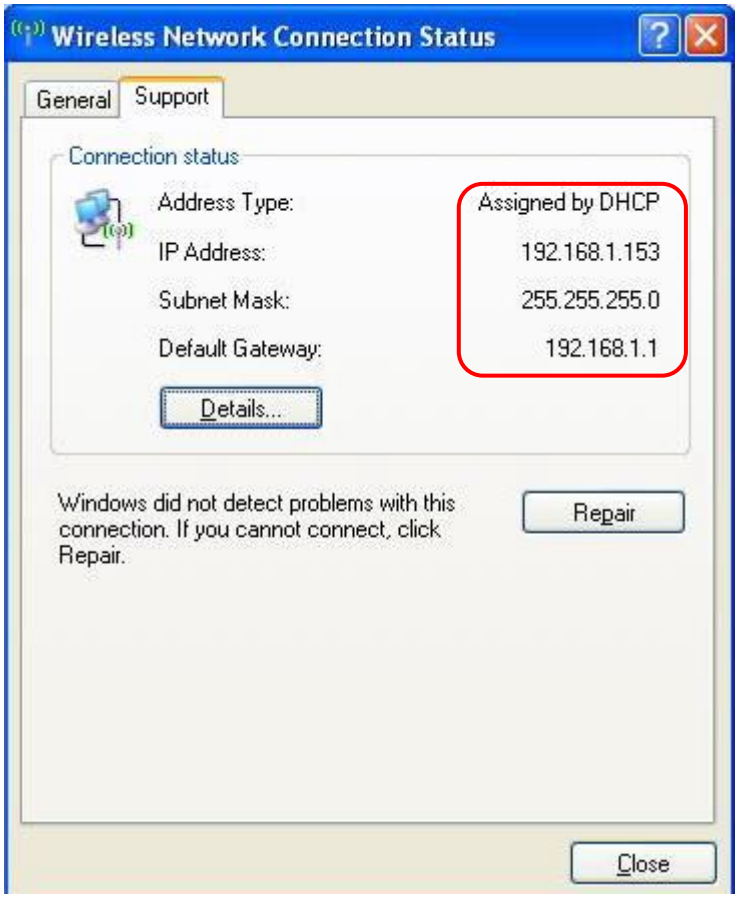
(5) Set “Broadcast SSID” to disable from page “Wireless Basic Setting”.



(6) Go to the upper level device WDS setting page and fill in the MAC address


WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.
Enable WDS
MAC Address: 000e68ff05do
Data Rate: Auto
Comment:
Please input the MAC address of this router.
Apply Changes
Reset
Set Security
Show Statistics
Current WDS AP List:
MAC Address
Tx Rate (Mbps)
Comment
Select
Delete Selected
Delete All
Reset

(7) You will receive an IP address from the upper lever device.



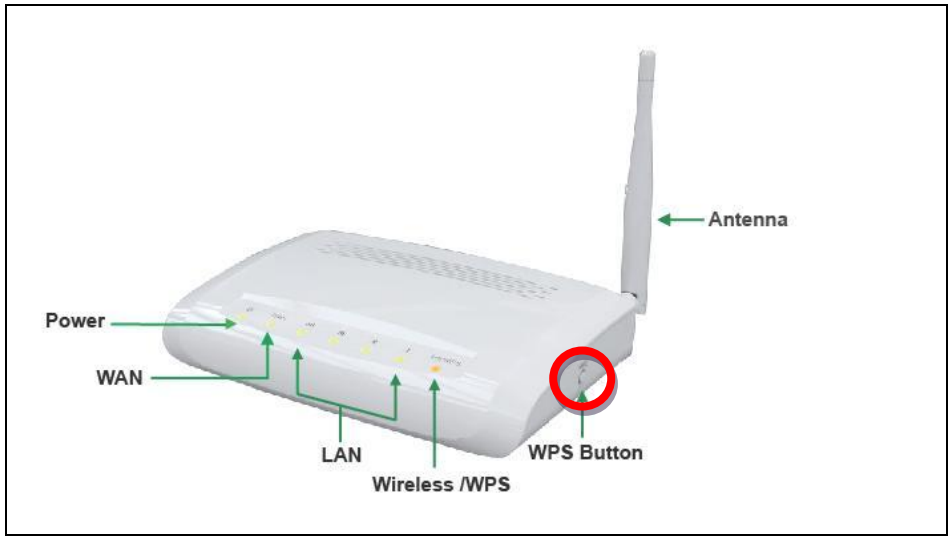
4.2.6 WPS

This page allows user to change the setting for WPS (*Wi-Fi Protected Setup*). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle. CBR-970/971 could support both Self-PIN or PBC modes, or use the WPS button (at real panel) to easy enable the WPS function.

PIN model, in which a PIN has to be taken either from a sticker label or from the web interface of the WPS device. This PIN will then be entered in the AP or client WPS device to connect.

PBC model, in which the user simply has to push a button, either an actual or a virtual one, on both WPS devices to connect.

Please find the WPS button from the following illustrate



When users select a specific model on wireless base station, the clients can connect to the base by selecting the same model.

The connection procedures of PIN and PBC are almost the same. The small difference between those two is:

Users input the PIN of wireless card in the base station first; it will limit the range of the clients. It is faster to establish a connection on PIN model.

On PBC model, users push the WPS button to activate the function, and then the wireless client must

push the WPS button in 2 minutes to enter the network. The client will search to see if there is any wireless base station which supports WPS is activating. If the client finds a matching base, the connection will be established. The speed of establishing a connection is slower than the PIN model because of this extra step.

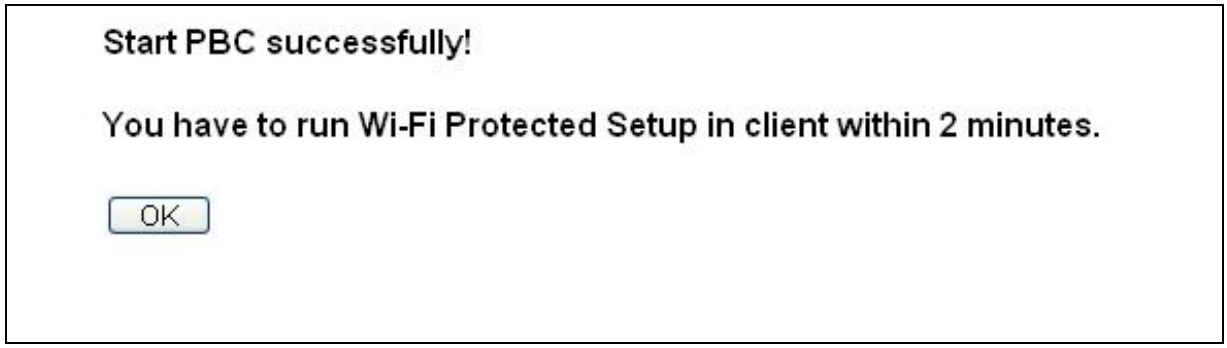
On the other hand, users need to input the information of the wireless card into the register interface. It might lead to the failure of connection, if users make mistakes on inputting. On PBC model, users only need to click the WPS button on both sides to make a connection. It is easier to operate.

This page supports **Start PBC** and **Start PIN**; please read the following instructions

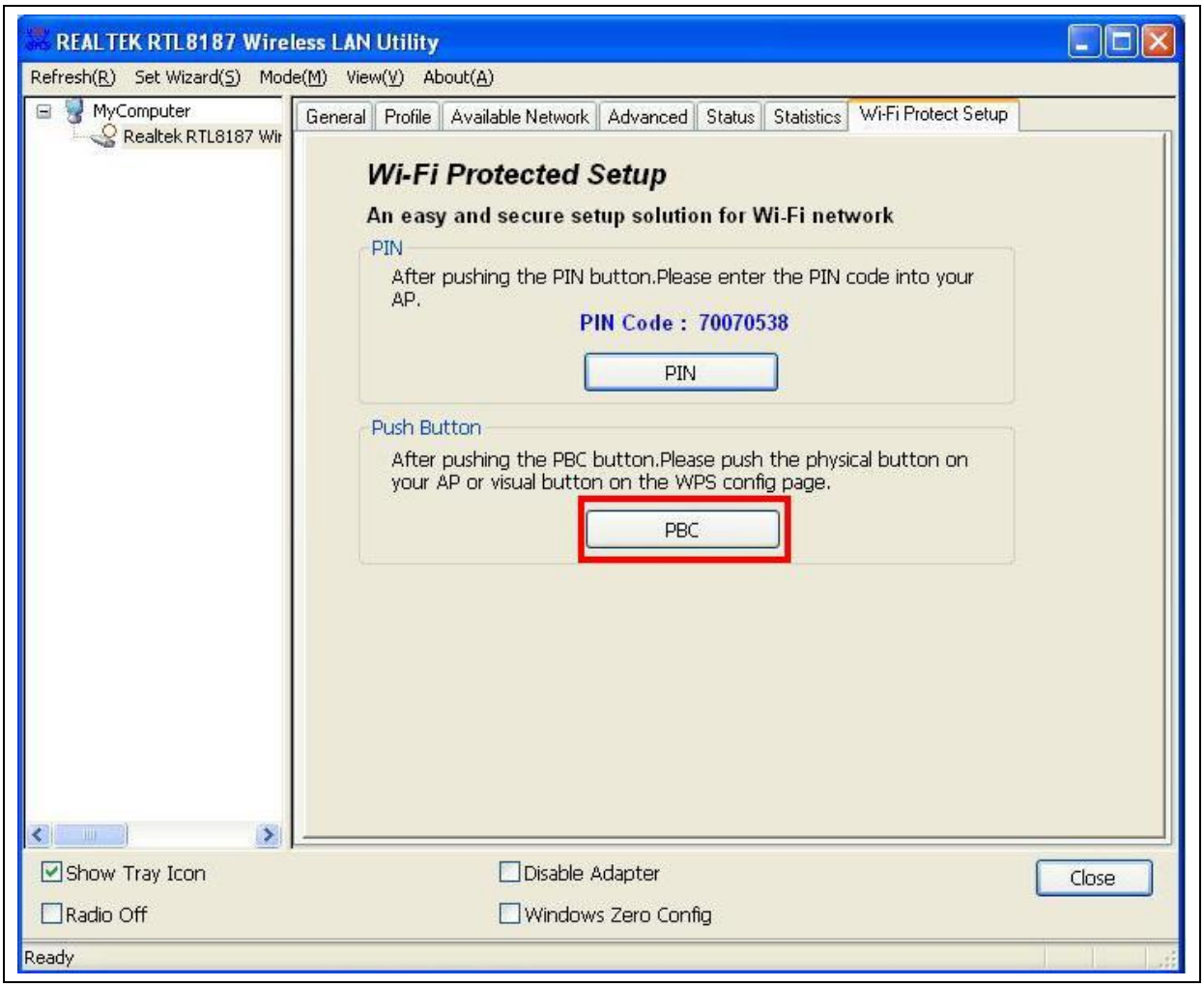
* Start PBC:

(1) Click **Start PBC** to connect to the wireless network card.

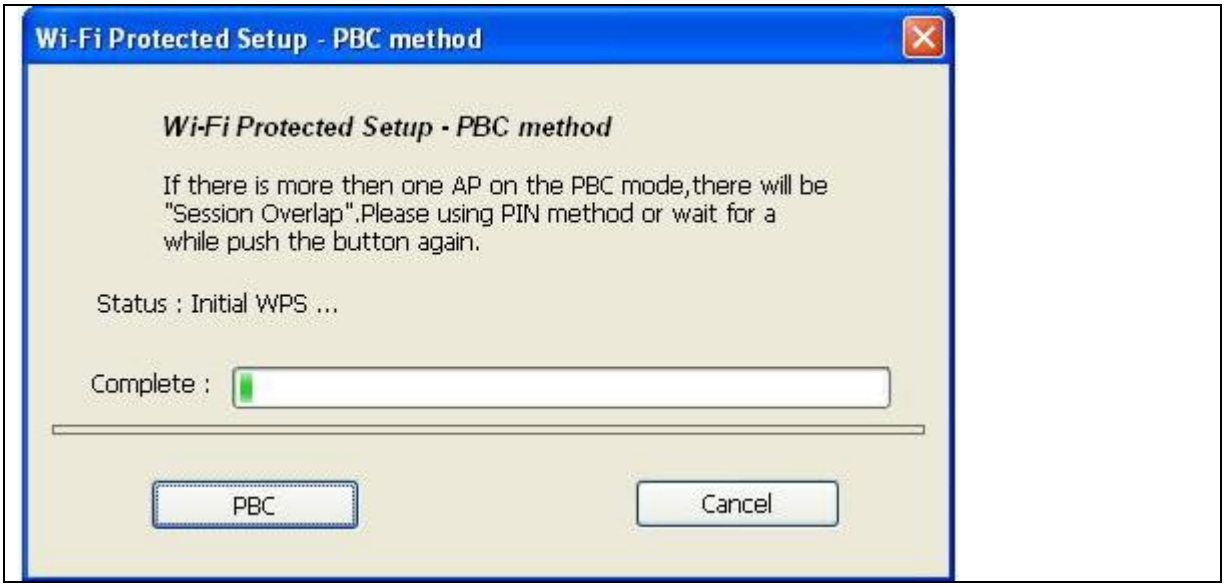
(2) Click **OK** to start WPS process.



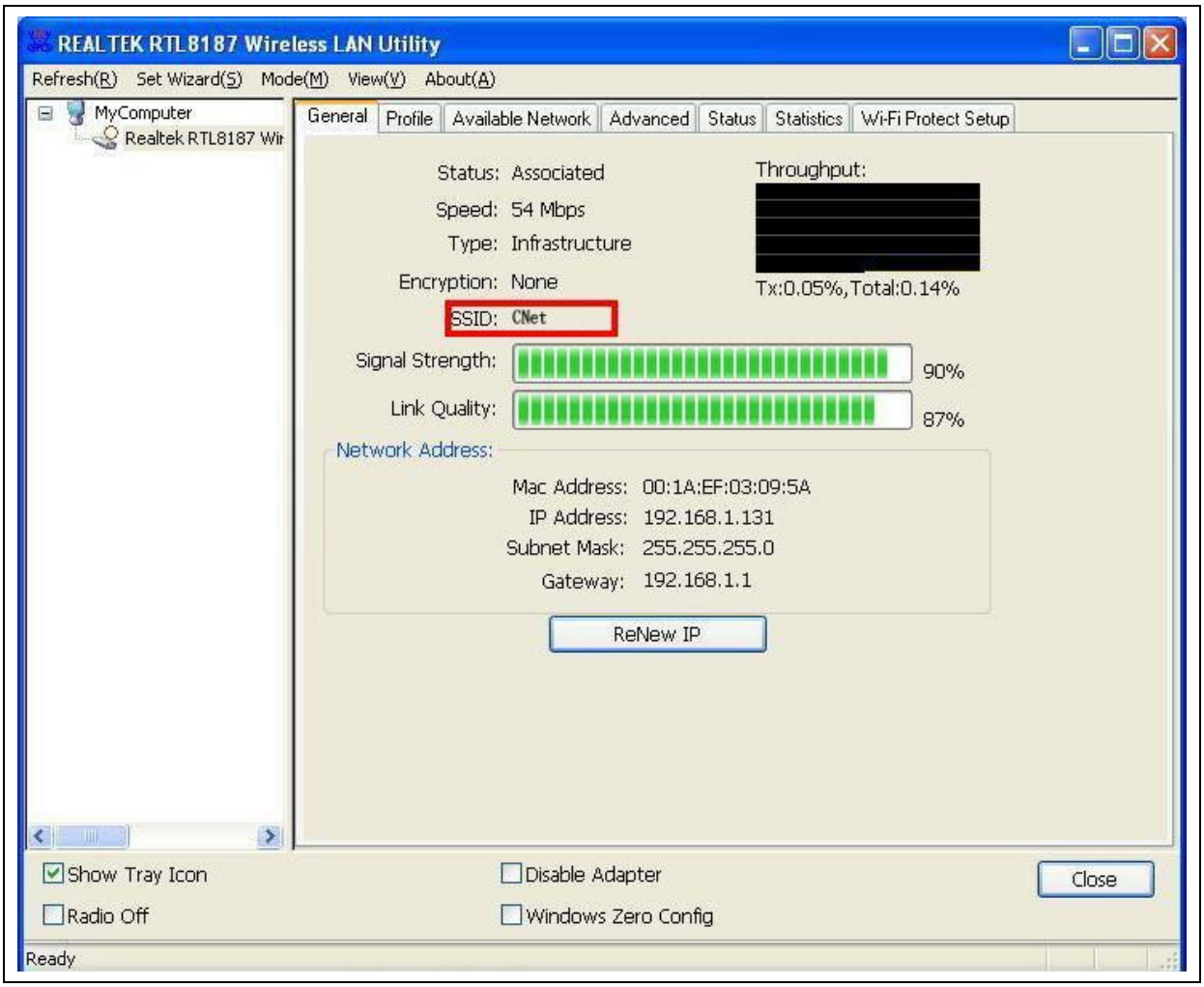
(3) Open the configuration page of the wireless card. Click the **Wi-Fi Protect Setup**, and then click **PBC** to start the WPS process.


REALTEK RTL8187 Wireless LAN Utility
Refresh(R) Set Wizard(S) Mode(M) View(V) About(A)
MyComputer
Realtek RTL8187 Wir
General Profile Available Network Advanced Status Statistics Wi-Fi Protect Setup
Wi-Fi Protected Setup
An easy and secure setup solution for Wi-Fi network
PIN
After pushing the PIN button.Please enter the PIN code into your AP.
PIN Code : 70070538
PIN
Push Button
After pushing the PBC button.Please push the physical button on your AP or visual button on the WPS config page.
PBC
Show Tray Icon
Disable Adapter
Close
Radio Off
Windows Zero Config
Ready

(4) The WPS is being processed.

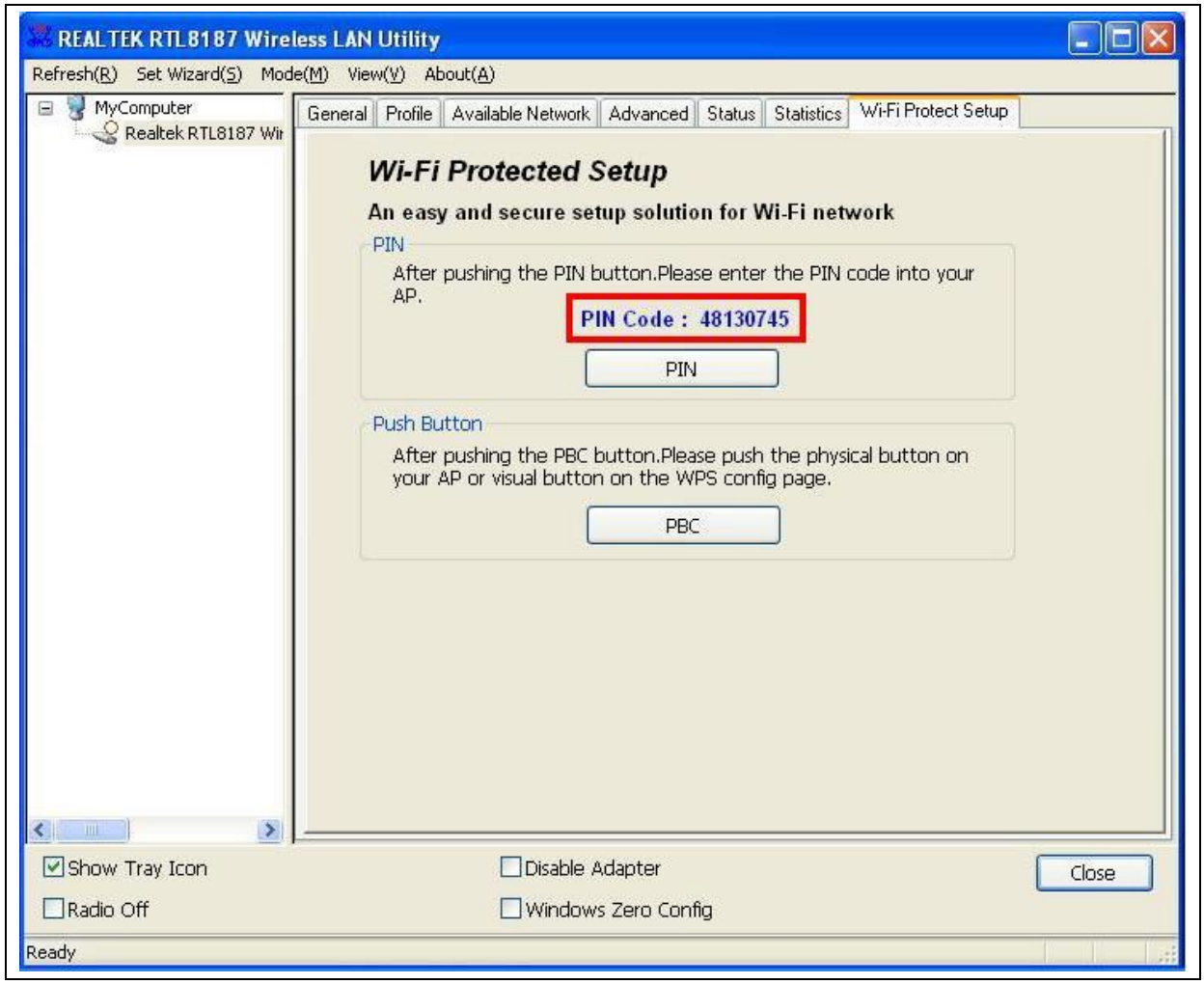

Wi-Fi Protected Setup - PBC method
Wi-Fi Protected Setup - PBC method
If there is more then one AP on the PBC mode,there will be "Session Overlap".Please using PIN method or wait for a while push the button again.
Status : Initial WPS ...
Complete :
PBC
Cancel

(5) The USB dongle will receive the connection information from wireless router if the dongle has connected to the wireless router successfully.

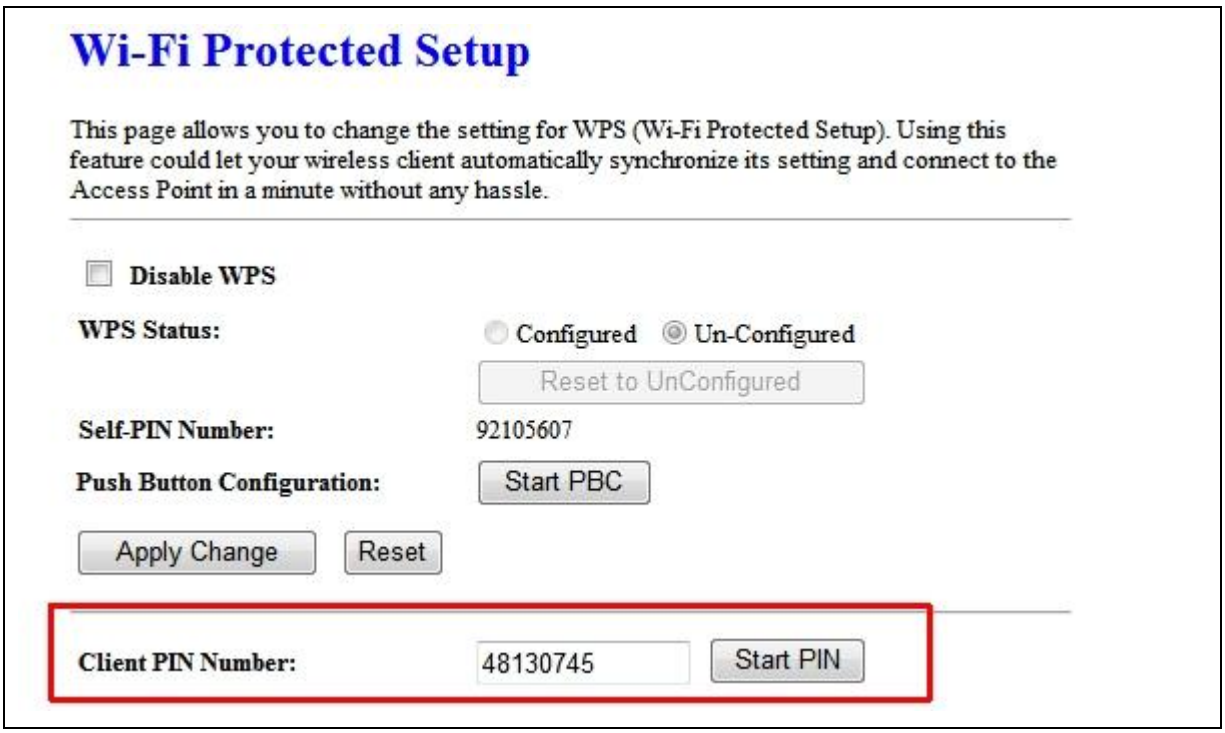


* Start PIN:

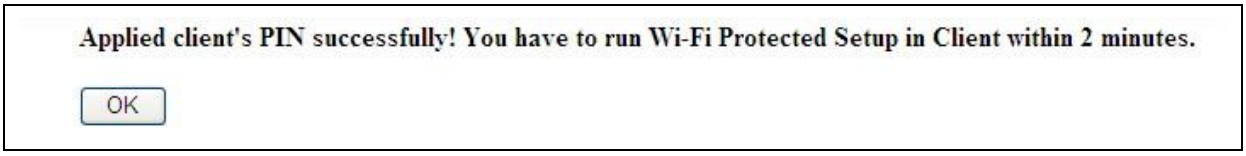
(1.) Get the WPS PIN number from wireless card and write it down.



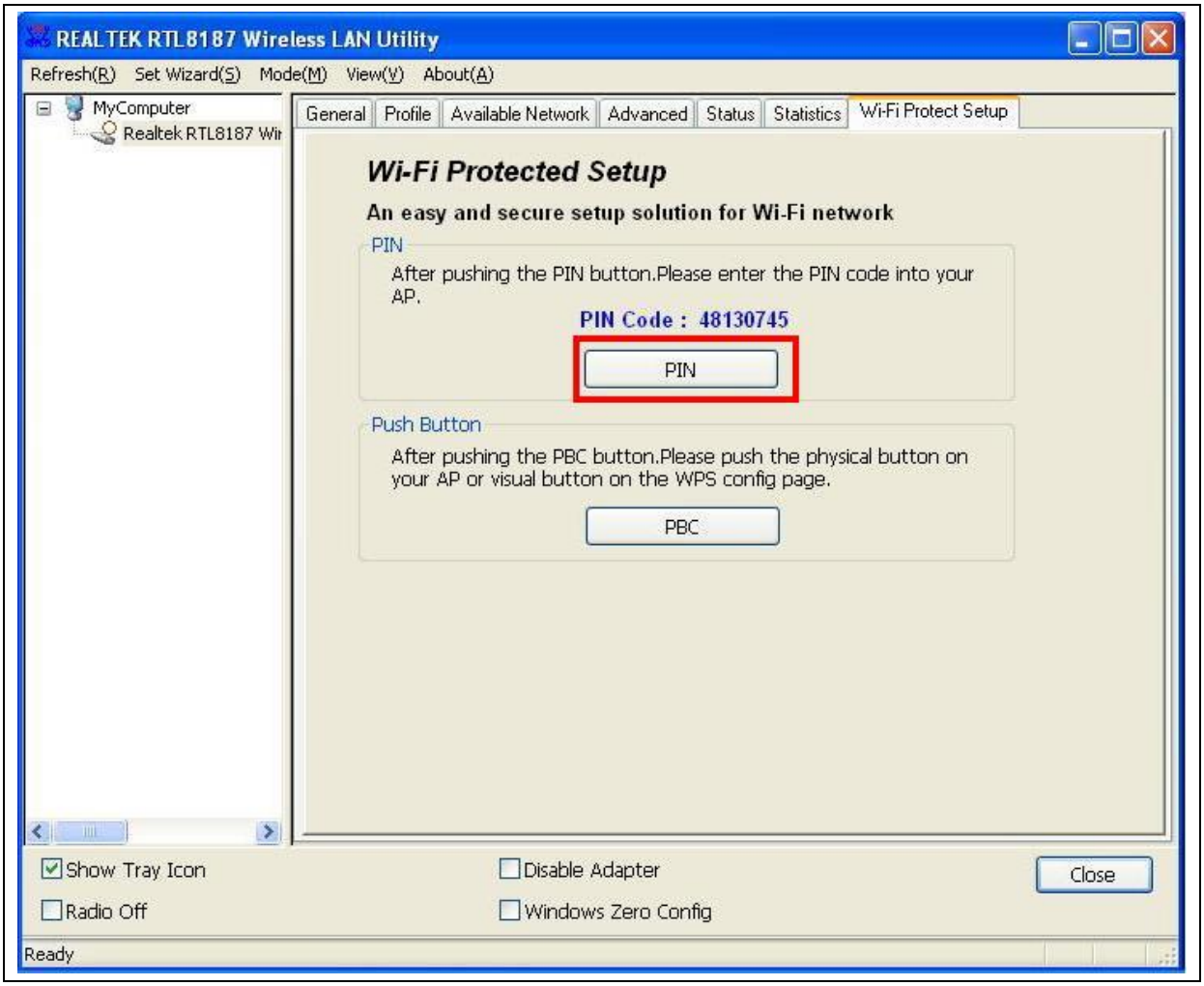
(2) Fill in the PIN number from the wireless card in Client PIN Number field, and then click “Start PIN”.


Wi-Fi Protected Setup
This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.
Disable WPS
WPS Status:
Configured
Un-Configured
Reset to UnConfigured
Self-PIN Number:
92105607
Push Button Configuration:
Start PBC
Apply Change
Reset
Client PIN Number:
48130745
Start PIN

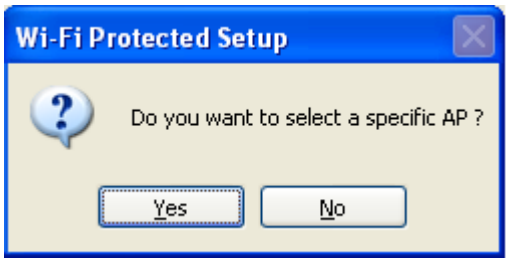
(3) Click **OK** to starts process.



(4) Click **PIN** to start the WPS process with the wireless router.


REALTEK RTL8187 Wireless LAN Utility
Refresh(R) Set Wizard(S) Mode(M) View(V) About(A)
MyComputer
Realtek RTL8187 Wir
General Profile Available Network Advanced Status Statistics Wi-Fi Protect Setup
Wi-Fi Protected Setup
An easy and secure setup solution for Wi-Fi network
PIN
After pushing the PIN button.Please enter the PIN code into your AP.
PIN Code : 48130745
PIN
Push Button
After pushing the PBC button.Please push the physical button on your AP or visual button on the WPS config page.
PBC
Show Tray Icon
Disable Adapter
Close
Radio Off
Windows Zero Config
Ready

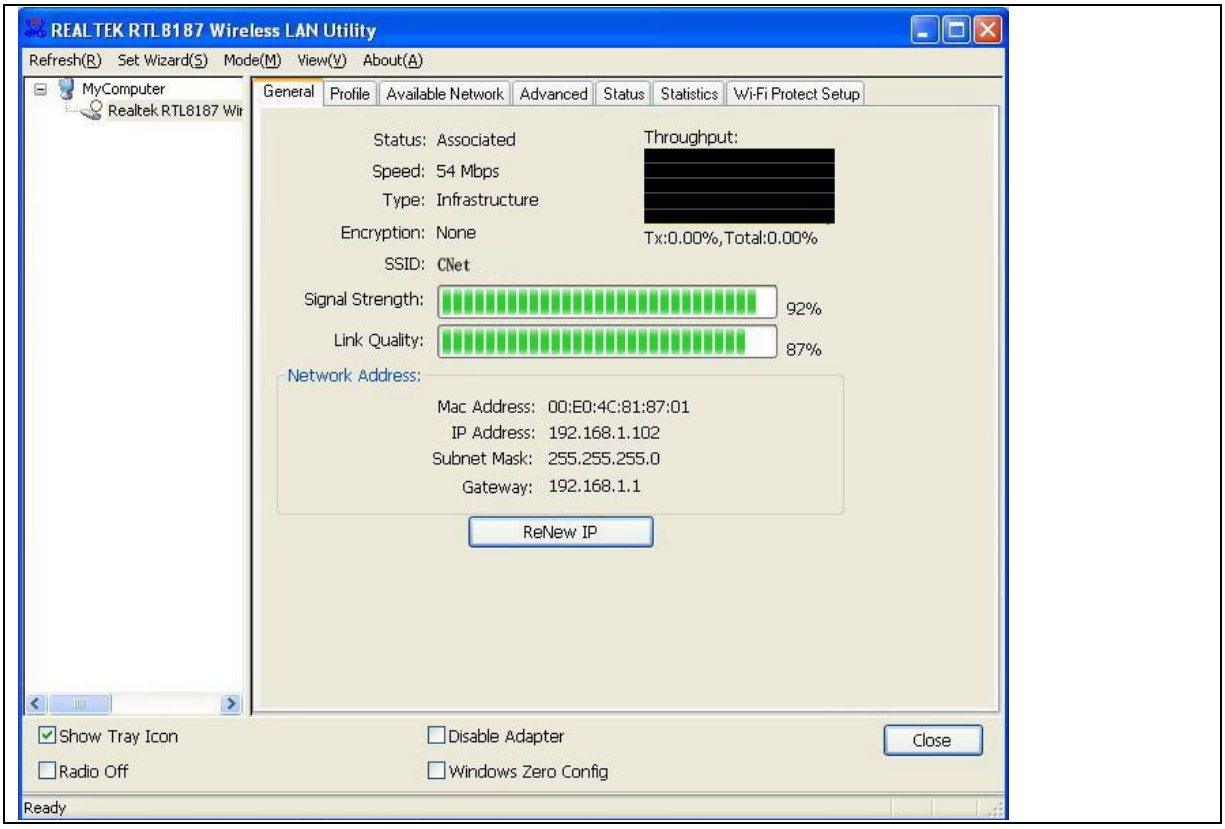
(5) Click **No,** then USB Dongle will select AP automatically.



(6) WPS is in processing.

Wi-Fi Protected Setup - PIN method
Wi-Fi Protected Setup - PIN method
Please enter the following PIN code into your AP .
PIN Code : 48130745
Status : Initial WPS ...
Cancel

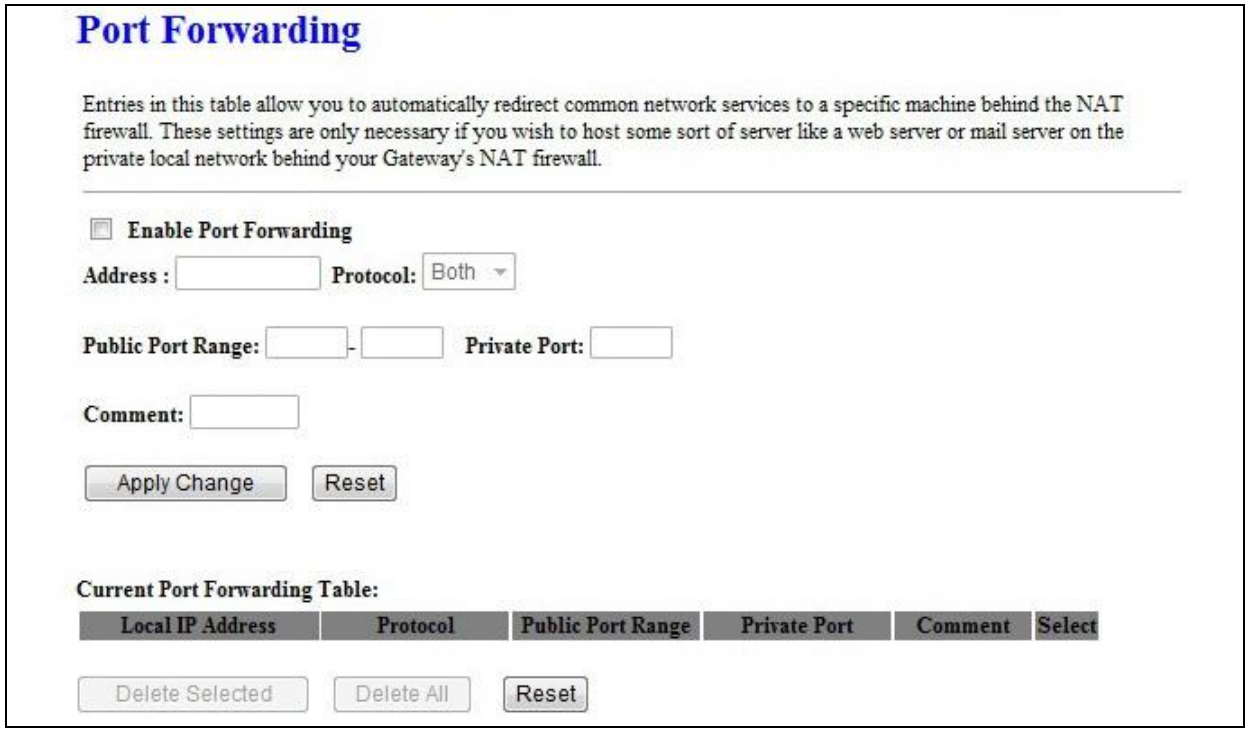
(7) The following page shows the wireless card has already connected to the wireless router.



4.3 NAT

4.3.1 Virtual Server

The Virtual Server feature allows users to create Virtual Servers by re-directing a particular range of service port numbers (from the WAN port) to a particular LAN IP address.


Port Forwarding
Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.
Enable Port Forwarding
Address :
Protocol: Both
Public Port Range: -
Private Port:
Comment:
Apply Change
Reset
Current Port Forwarding Table:
Local IP Address
Protocol
Public Port Range
Private Port
Comment
Select
Delete Selected
Delete All
Reset

Item	Description
Enable Port Forwarding	Select to enable Port Forwarding service or not.
IP Address	Specify the IP address which receives the incoming packets.
Protocol	Select the protocol type.
Port Range	Enter the port number, for example 80-80 or 20-22
Comment	Add comments for this port forwarding rule.
Apply Change & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.
Current Port Forwarding Table	It will display all port forwarding regulation you made.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.
Reset	Click **Reset** to cancel.

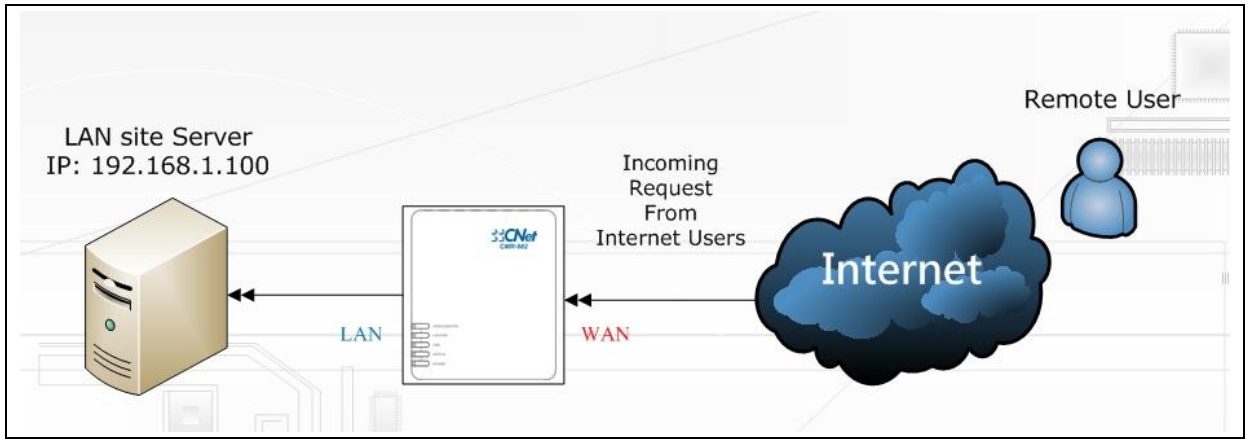
*Please find the following figure to know that what the virtual server is. The web server is located on 192.168.1.100, forwarding port is 80, and type is TCP+UDP.

Configuration:

Private IP: 192.168.1.100

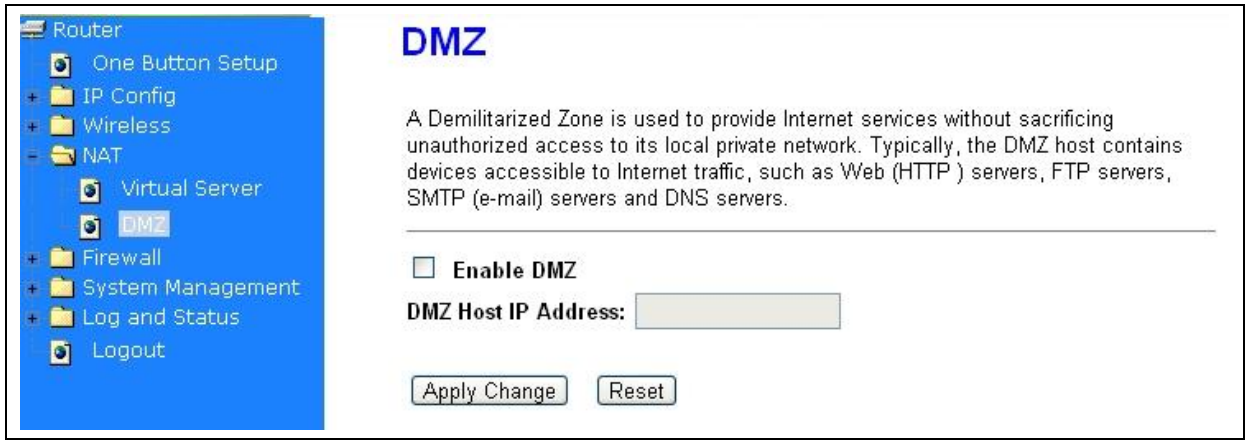
Port: 80 - 80

Type: TCP+UDP



4.3.2 DMZ

The DMZ feature allows one local user to be exposed to the Internet for special-purpose applications like Internet gaming or videoconferencing. When enabled, this feature opens all ports to a single station and hence renders that system exposed to intrusion from outside. The port forwarding feature is more secure because it only opens the ports required by that application.


Router
One Button Setup
IP Config
Wireless
NAT
Virtual Server
DMZ
Firewall
System Management
Log and Status
Logout
DMZ
A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.
Enable DMZ
DMZ Host IP Address:
Apply Change
Reset

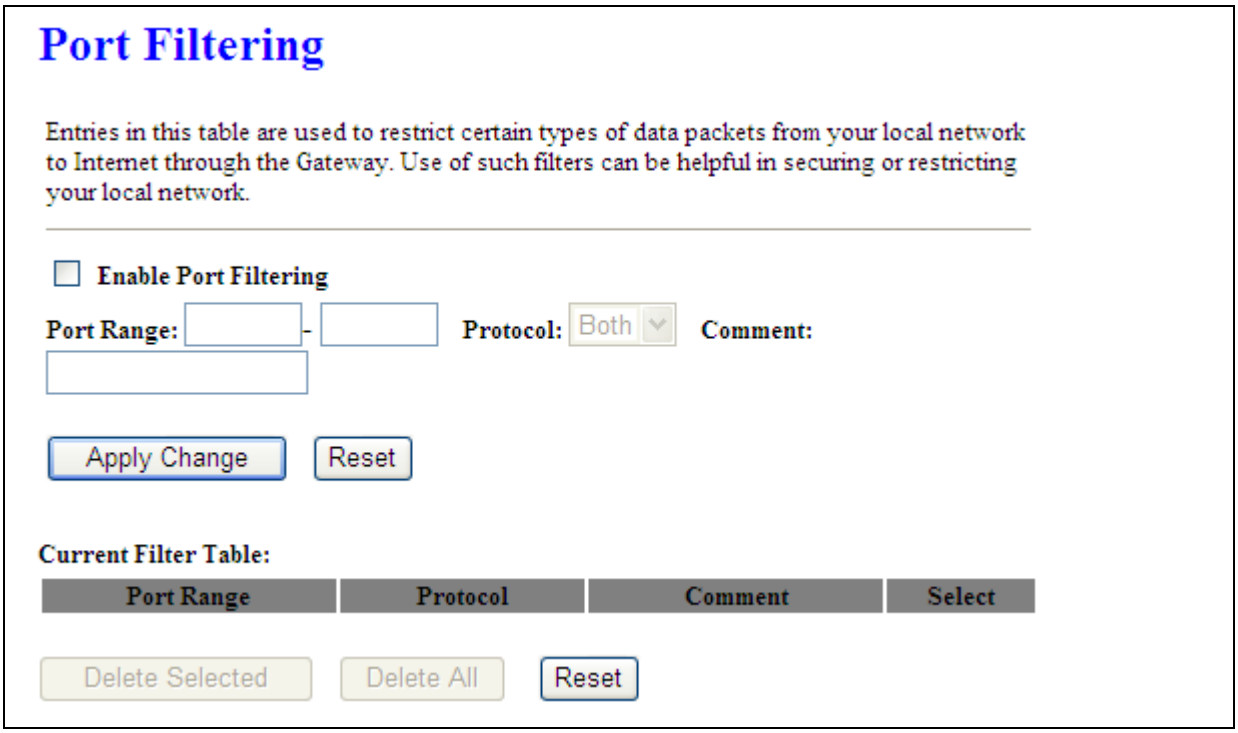
Item	Description
Enable DMZ	It will enable the DMZ service if you select it.

DMZ Host IP Address	Please enter the specific IP address for DMZ host.
Apply Change & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

4.4 Firewall

4.4.1 Port Filtering

When enabled packets are denied access to Internet/filtered based on their port address.

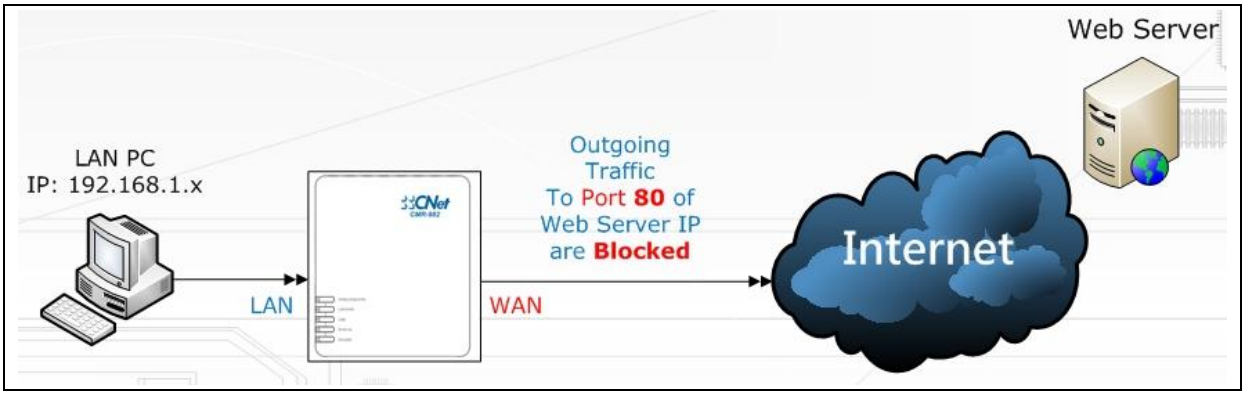


Item	Description
Enable Port Filtering	Please select **Enable Port Filtering** to filter ports.
Port Range	Please enter the port number that needs to be filtered.
Protocol	Please select the protocol type of the port.
Comment	You can add comments for this regulation.
Apply Change & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.
Rest	You can click **Reset** to cancel.

* Port 80 has been blocked as the following illustrate.

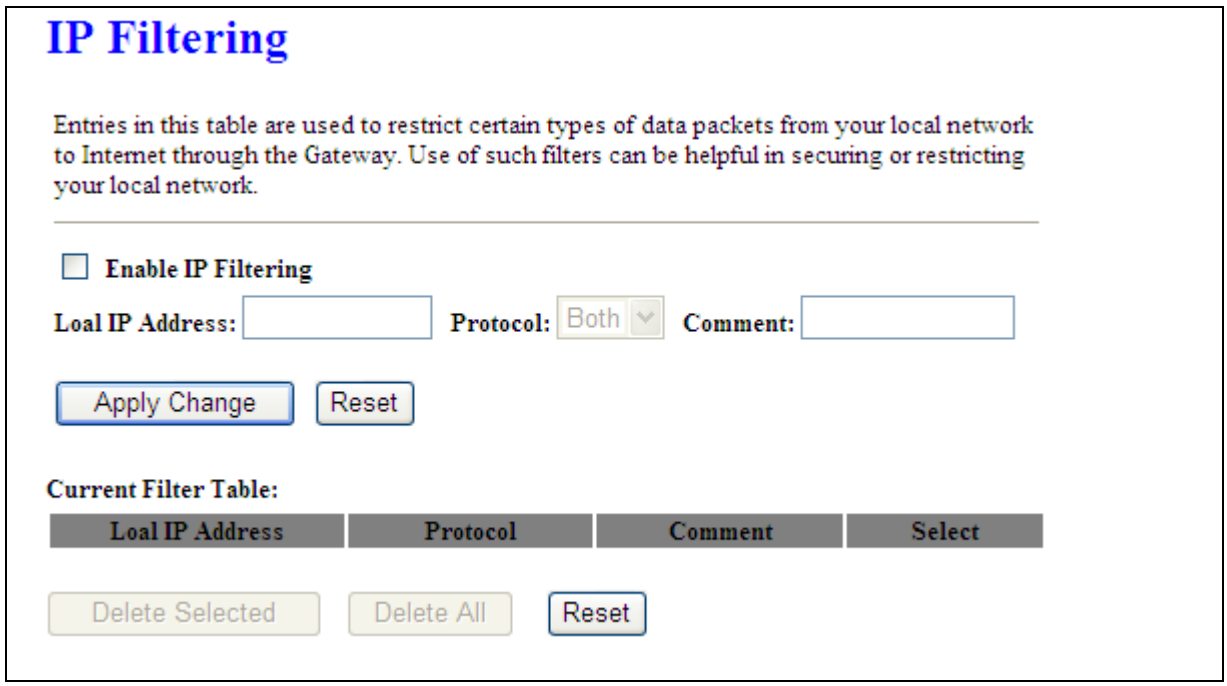
IP: 192.168.1.X

Port: 80-80



4.4.2 IP Filtering

When enabled, LAN clients are blocked / filtered from accessing the Internet based on their IP addresses.

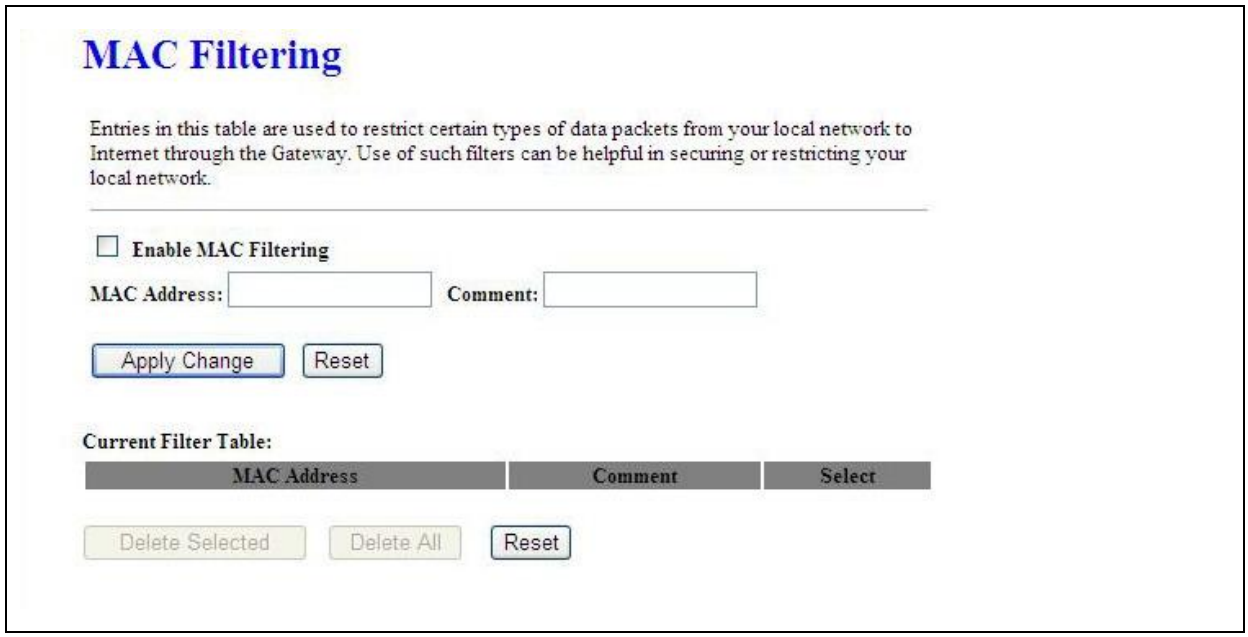


Item	Description
Enable IP Filtering	Please select **Enable IP Filtering** to filter IP addresses.
Local IP Address	Please enter the IP address that needs to be filtered.
Protocol	Please select the protocol type of the IP address.
Comment	You can add comments for this regulation.
Apply Change & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.
Current Filter Table	It will display all ports that are filtering now.

Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.
Rest	You can click **Reset** to cancel.

4.4.3 MAC Filtering

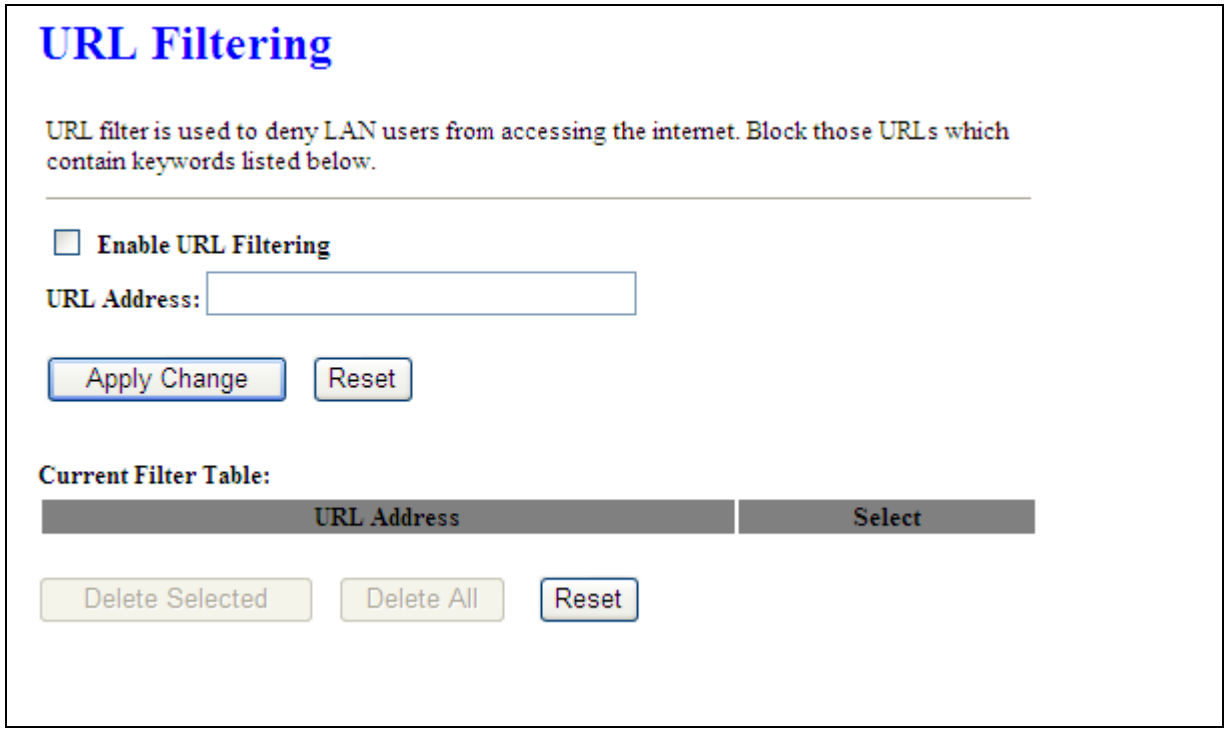
When enabled, filtering will be based on the MAC address of LAN computers. Any computer with its MAC address on this list will be blocked from accessing the Internet.


MAC Filtering
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.
Enable MAC Filtering
MAC Address:
Comment:
Apply Change
Reset
Current Filter Table:
MAC Address
Comment
Select
Delete Selected
Delete All
Reset

Item	Description
Enable MAC Filtering	Please select **Enable MAC Filtering** to filter MAC addresses
MAC Address	Please enter the MAC address that needs to be filtered.
Comment	You can add comments for this regulation.
Apply Change & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.
Rest	You can click **Reset** to cancel.

4.4.4 URL Filtering

URL Filtering is used to restrict users to access specific websites in internet



Item	Description
Enable URL Filtering	Please select **Enable MAC Filtering** to filter MAC addresses
URL Address	Please enter the MAC address that needs to be filtered.
Apply Change & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.
Current Filter Table	It will display all ports that are filtering now.
Delete Selected & Delete All	Click **Delete Selected** will delete the selected item. Click **Delete All** will delete all items in this table.
Rest	You can click **Reset** to cancel.

Notes: This function will not be in effect when the Virtual Server is enabled. Please disable Virtual Server before activate the URL Filtering function.

4.5 System Management

It has 6 sections: Change Password, Firmware Upgrade, Profiles Save, Time Zone Setting, UPnP Setting, and Language Setting. It is easy and helpful for users making more detailed settings.

4.5.1 Change Password

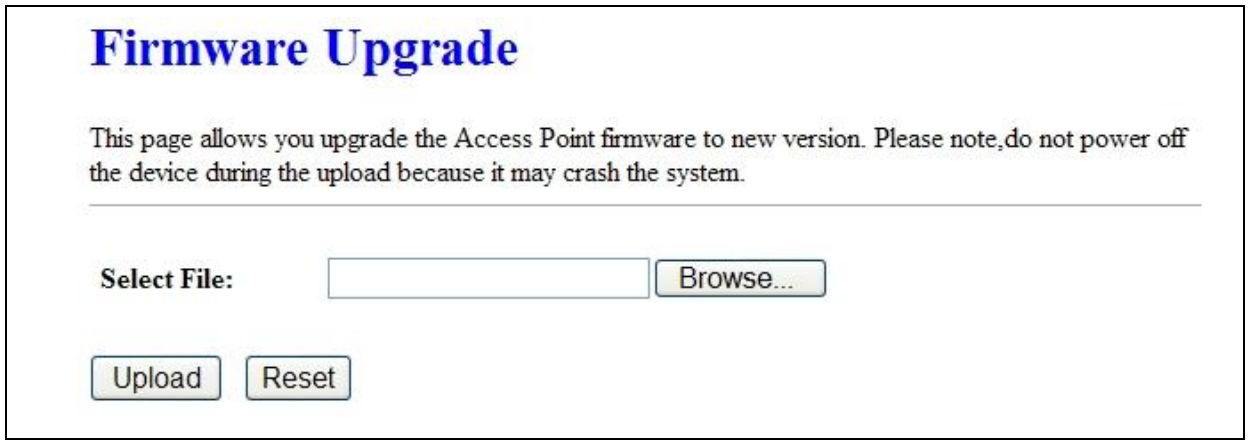
Users can set or change user name and password used for accessing the web management interface in this section.

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

4.5.2 Firmware Upgrade

The firmware on this wireless router can be easily upgraded. You can check the website (http://www.cnet.com.tw) to see if there is any later version of firmware

Notes: Do not power off the device while the firmware is being upgraded

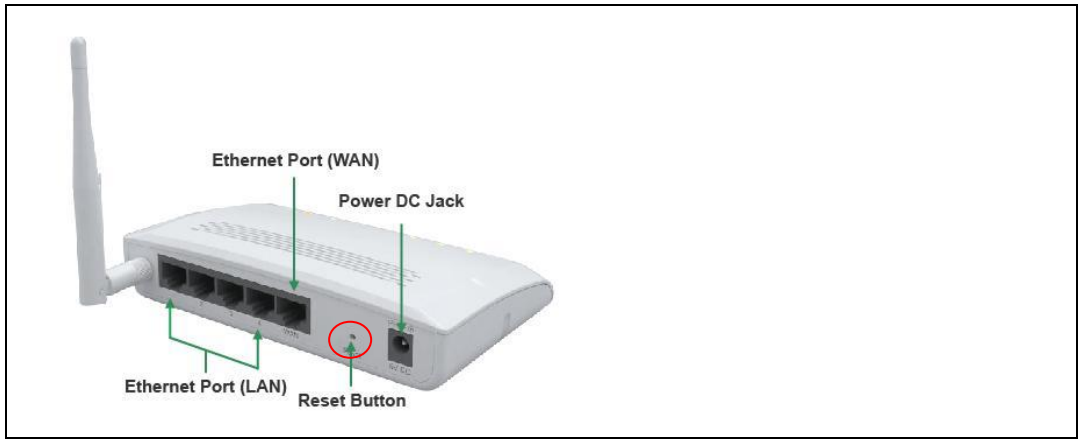

Firmware Upgrade
This page allows you upgrade the Access Point firmware to new version. Please note,do not power off the device during the upload because it may crash the system.
Select File:
Browse...
Upload
Reset

Caution: To prevent that firmware upgrading is interrupted by other wireless signals and causes failure. We recommend users to use wired connection during upgrading.

Caution: The firmware upgrade will not remove your previous settings.

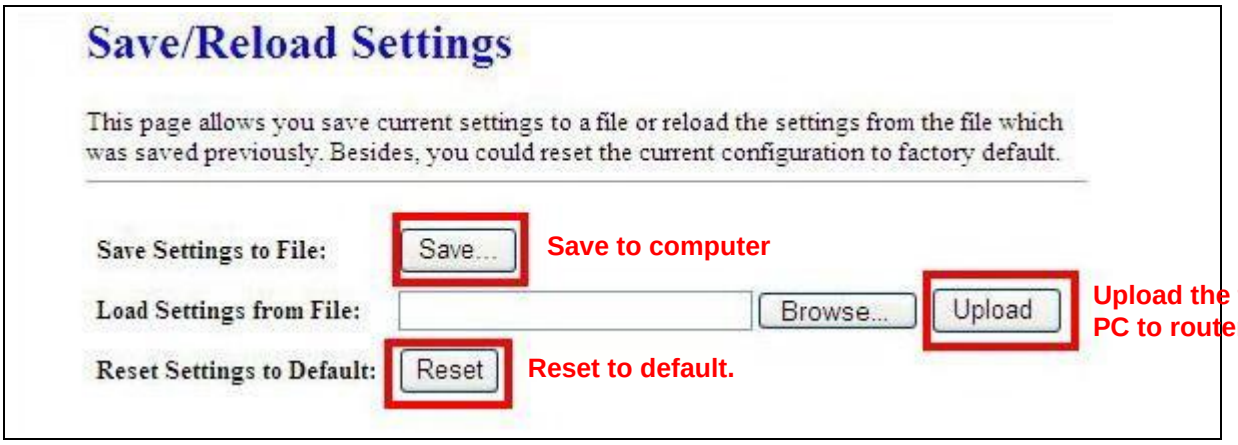
***Reset button**:

On the front of this router, there is a reset button. If you cannot login the administrator page by forgetting your password; or the router has problem you can't solve. You can push the reset button for 5 seconds with a stick. The router will reboot and all settings will be restored to factory default settings. If the problem still exists, you can visit our web site to see if there is any firmware for download to solve the problem.



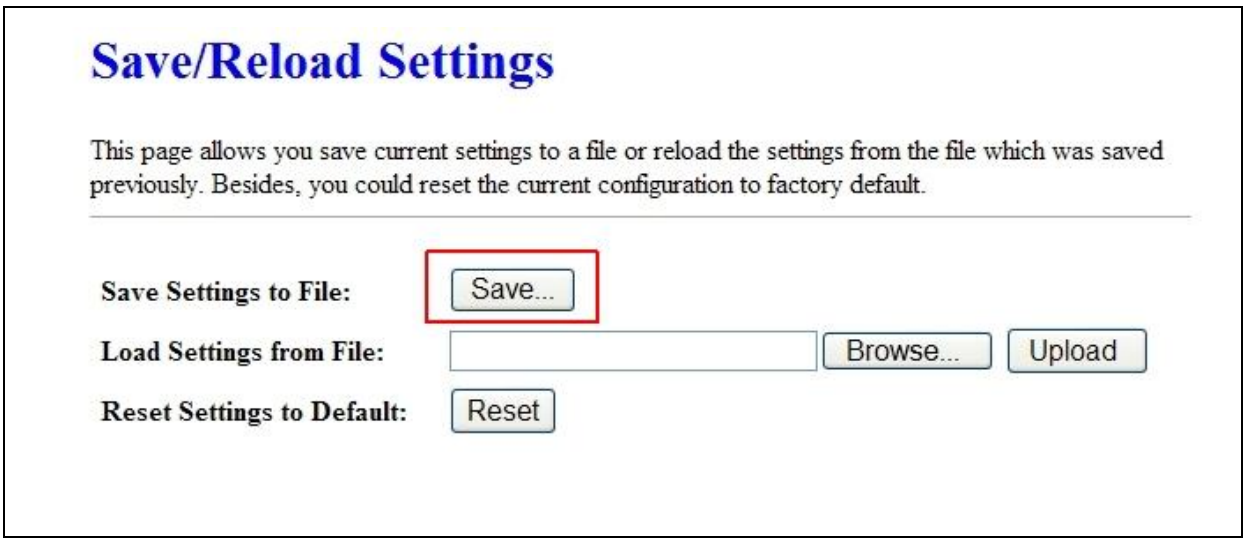
4.5.3 Profile Save

Users can create a backup file that contains current router settings. This backup file can be used to restore router settings. This is especially useful in the event you need to reset the router to its default settings.

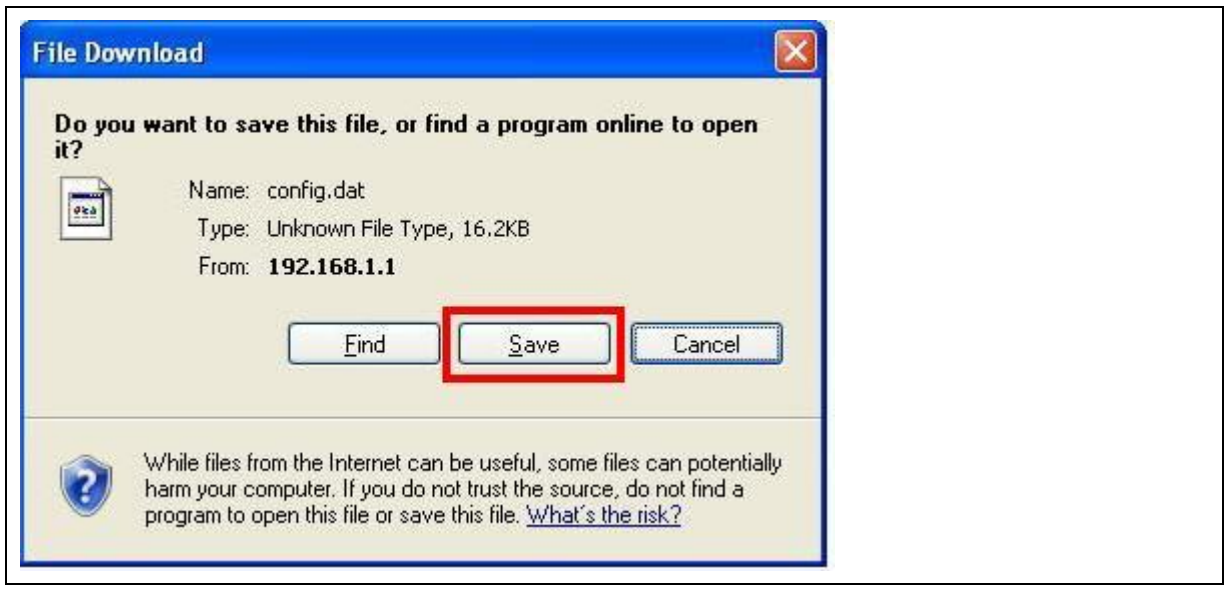

Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Save to computer
Load Settings from File:
Browse...
Upload
Upload the file from PC to router
Reset Settings to Default:
Reset
Reset to default.

a. Save Configuration

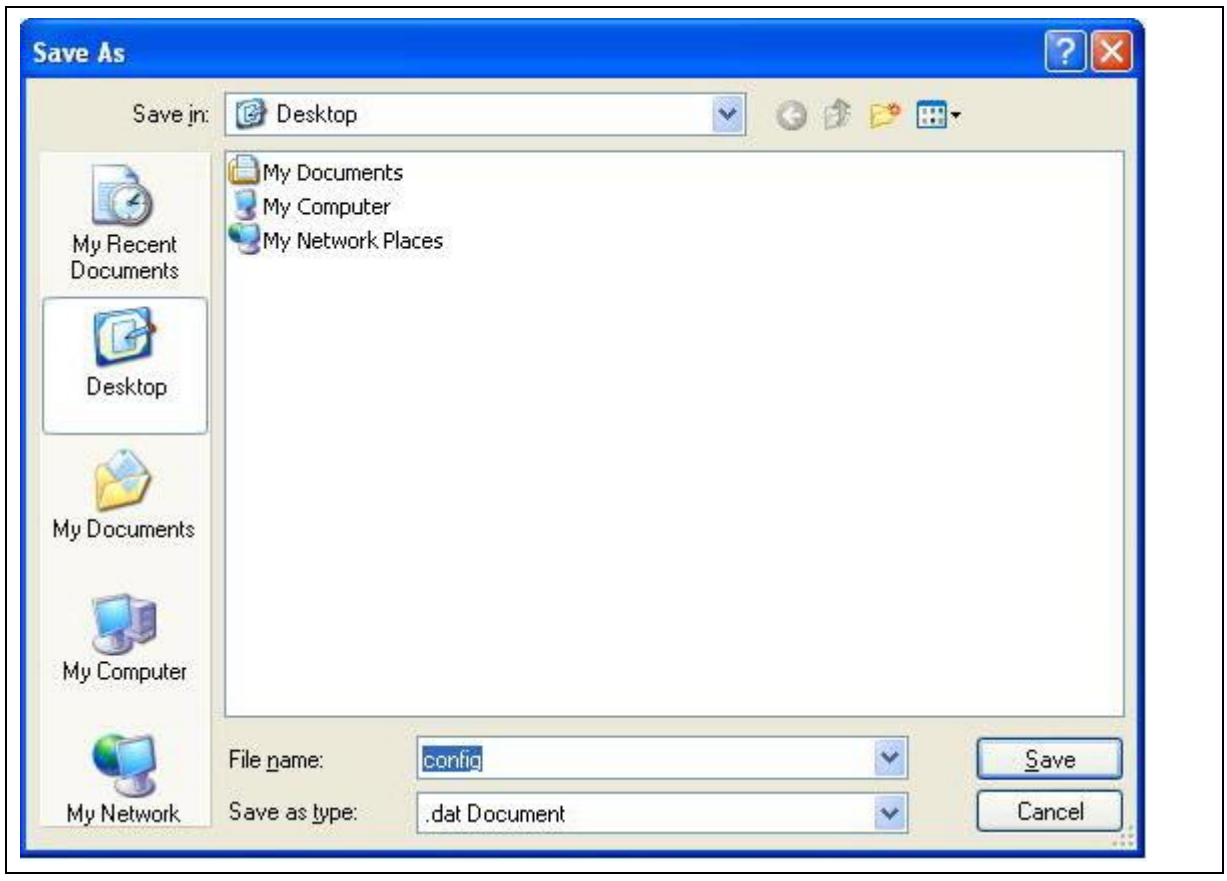
(1) Click **Save**


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Browse...
Upload
Reset Settings to Default:
Reset

(2) Please click “Save” to save the configuration to your computer.

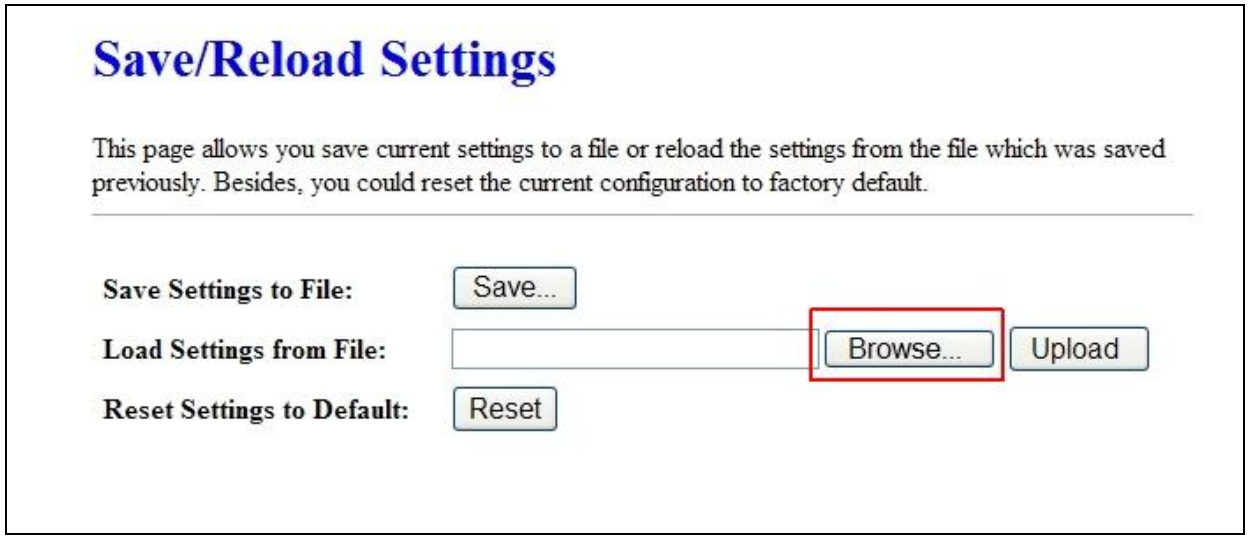

File Download
Do you want to save this file, or find a program online to open it?
Name: config.dat
Type: Unknown File Type, 16.2KB
From: 192.168.1.1
Find
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

(3) Select the location which you want to save file, then click **Save.**

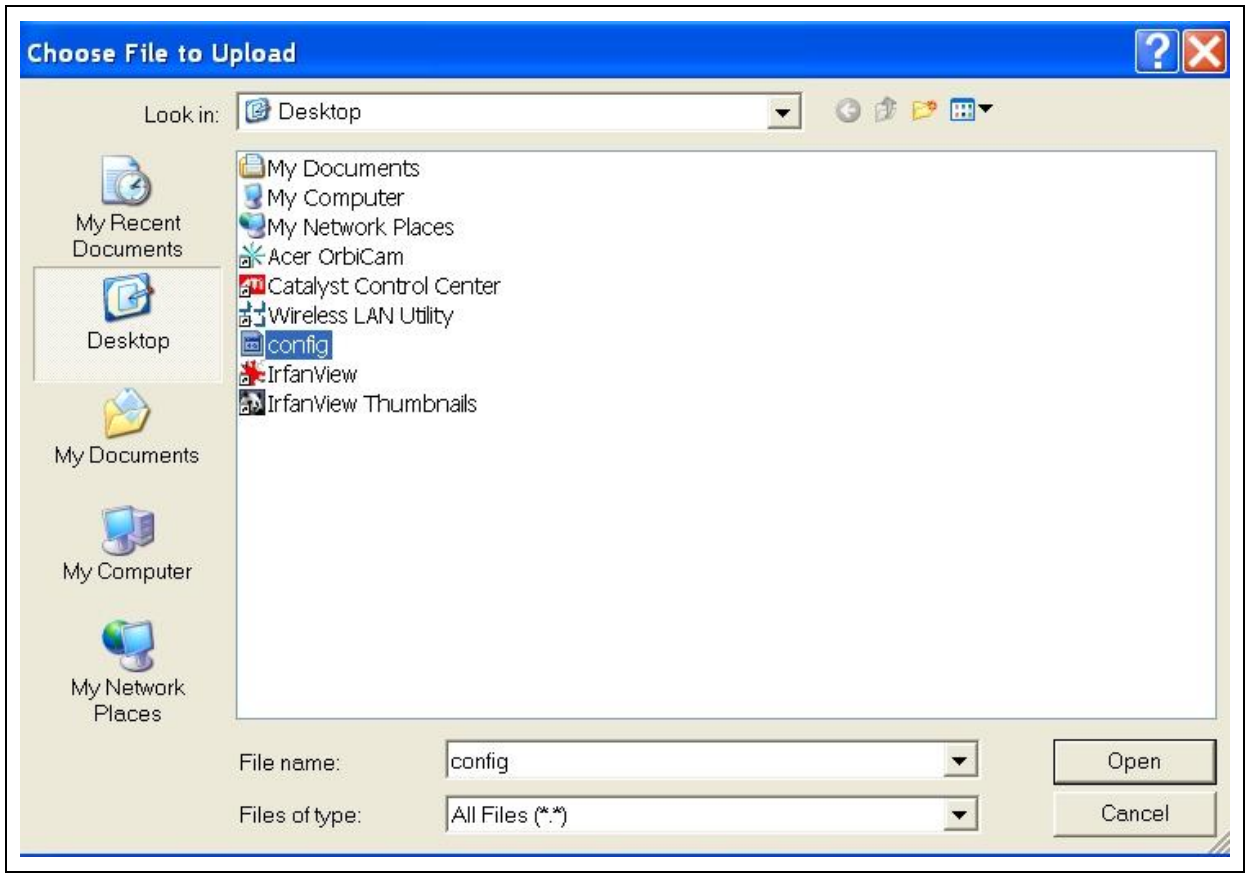


b. Load configuration file

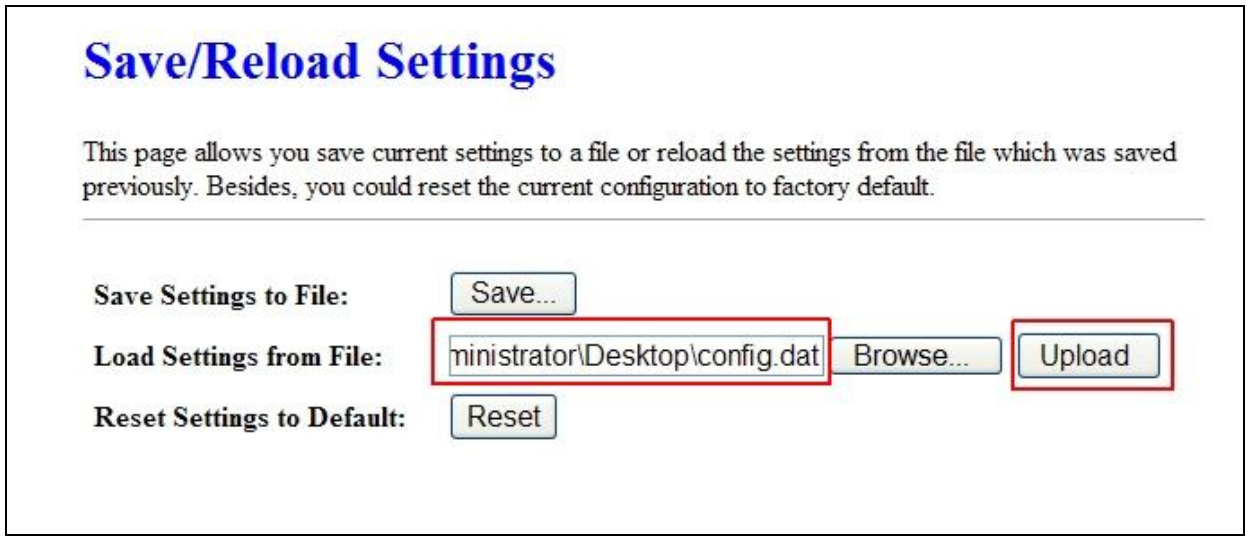
(1) Click **Browser**


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Browse...
Upload
Reset Settings to Default:
Reset

(2) Select configuration file then click **Open**



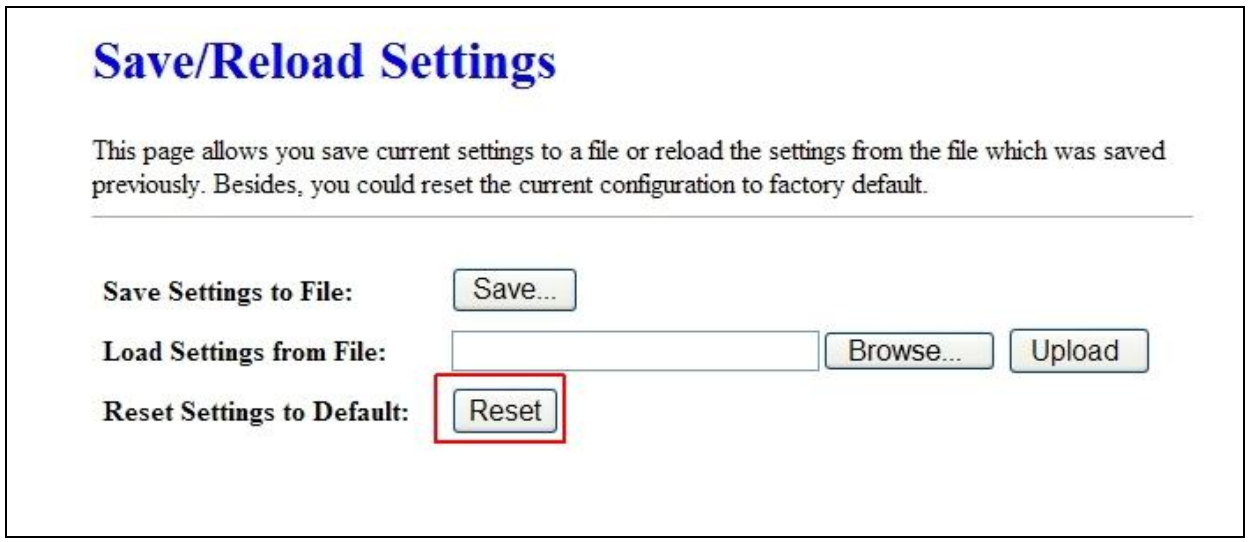
(3) Click **Upload** to upload configuration file to CBR-970/971.


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
ministrator\Desktop\config.dat
Browse...
Upload
Reset Settings to Default:
Reset

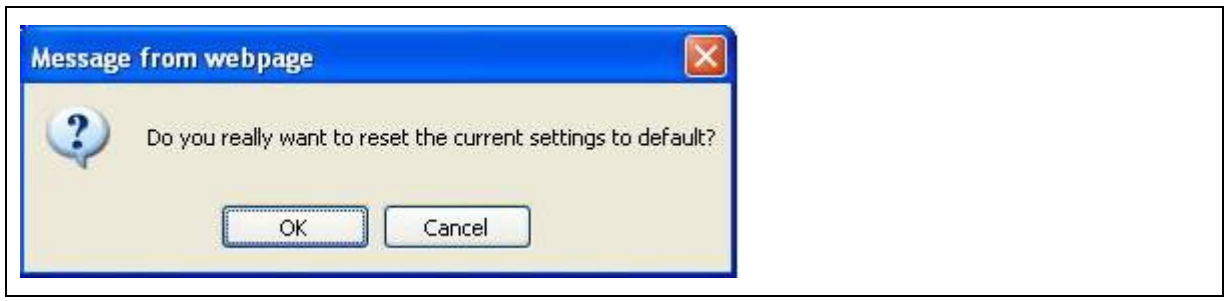
(4) After 90 seconds, CBR-970/971 will reboot automatically.

(C) Reload factory default setting

1. Please click **Reset**


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Browse...
Upload
Reset Settings to Default:
Reset

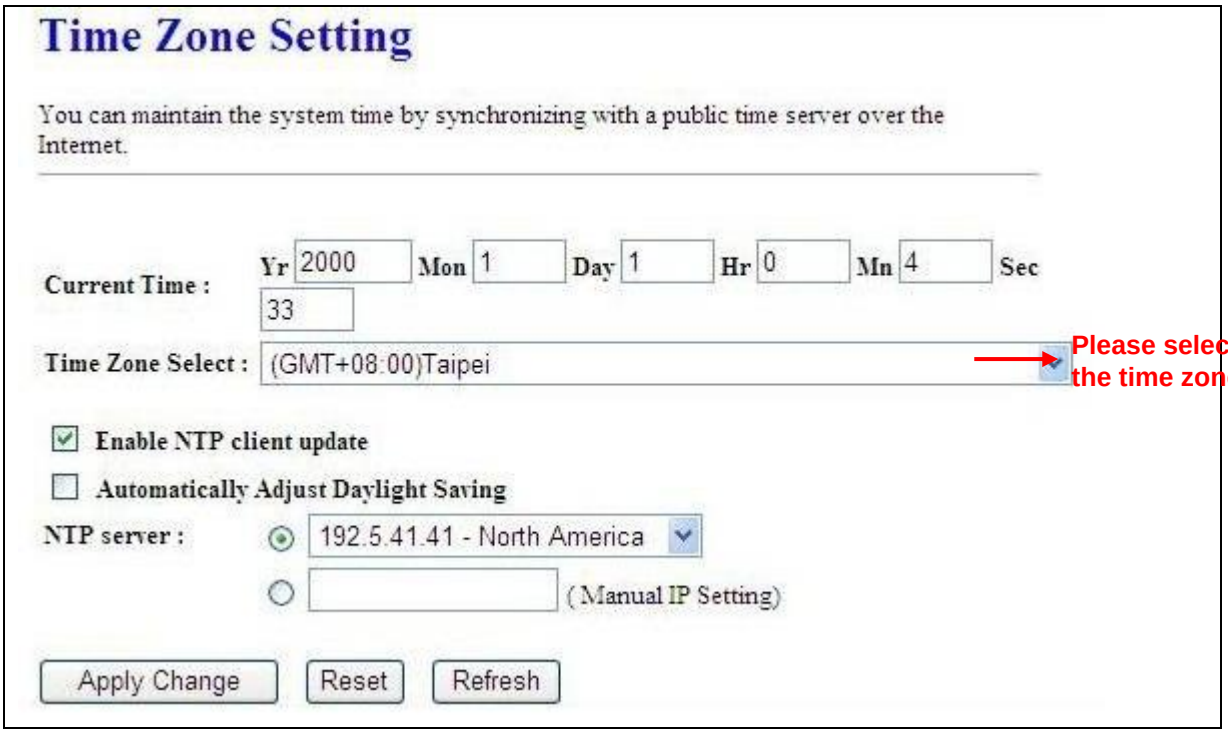
(2) Please click **OK** to start reload factory default setting to CBR-970/971.



(3) After 90 seconds, CBR-970/971 will reboot automatically.

4.5.4 Time Zone Setting

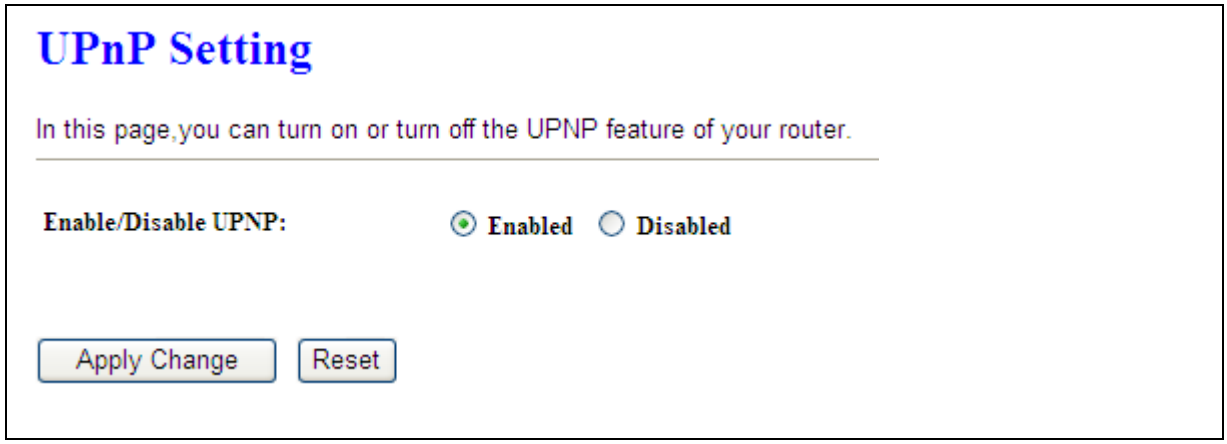
Users can synchronize the local clock on the router to an available NTP server (optional). To complete this setting, enable NTP client update and select the correct Time Zone.


Time Zone Setting
You can maintain the system time by synchronizing with a public time server over the Internet.
Current Time :
Yr 2000 Mon 1 Day 1 Hr 0 Mn 4 Sec 33
Time Zone Select :
(GMT+08:00)Taipei
Please select the time zone
Enable NTP client update
Automatically Adjust Daylight Saving
NTP server :
192.5.41.41 - North America
(Manual IP Setting)
Apply Change
Reset
Refresh

Item	Description
Current Time	Users can input the time manually.
Time Zone Select	Please select the time zone.
Enable NTP client update	Please select to enable NTP client update or not.
Automatically Adjust Daylight Saving	Please select to enable **Automatically Adjust Daylight Saving** or not.
NTP Server	Please select the NTP server from the pull-down list, or you can enter the NTP server IP address manually.
Apply Changes & Reset & Refresh	Please click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data. Or you may click on **Refresh** to update the system time on the screen.

4.5.5 UPnP Setting

Universal Plug and Play (**UPnP**) is a standard of networking protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. CBR-970/971 supports UPnP function, and can cooperate with other UPnP devices. When you activate UPnP, please click **My Network Places**. Users will see an **Internet Gateway Device** icon. By click the icon, users can enter the GUI of the router. If you do not wish to use UPnP, you can disable it.

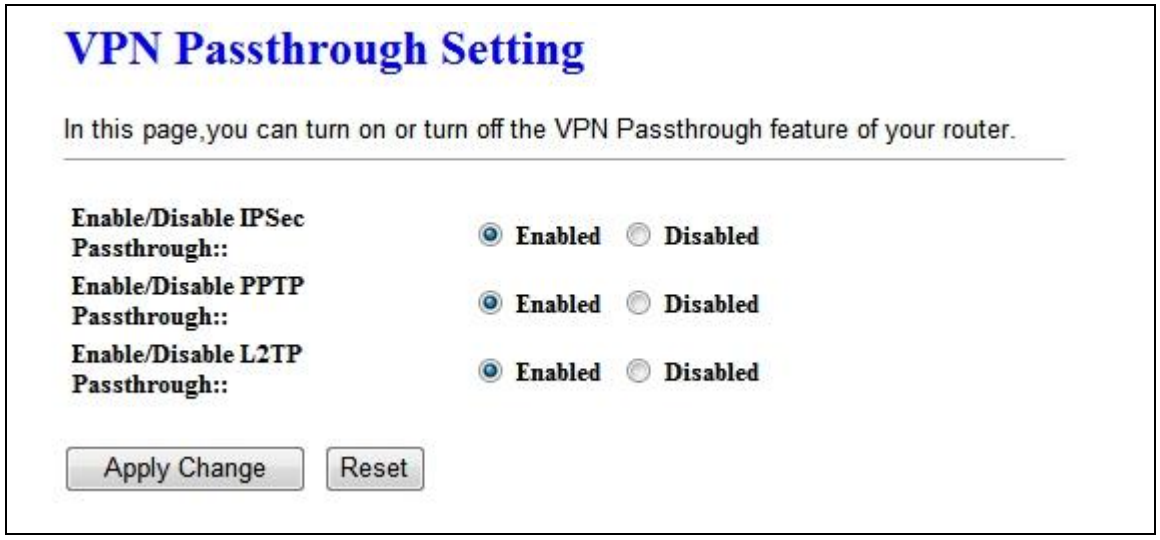


*Enable/Disable UPnP

Select to enable or disable this function.

4.6 VPN Passthrough Settings

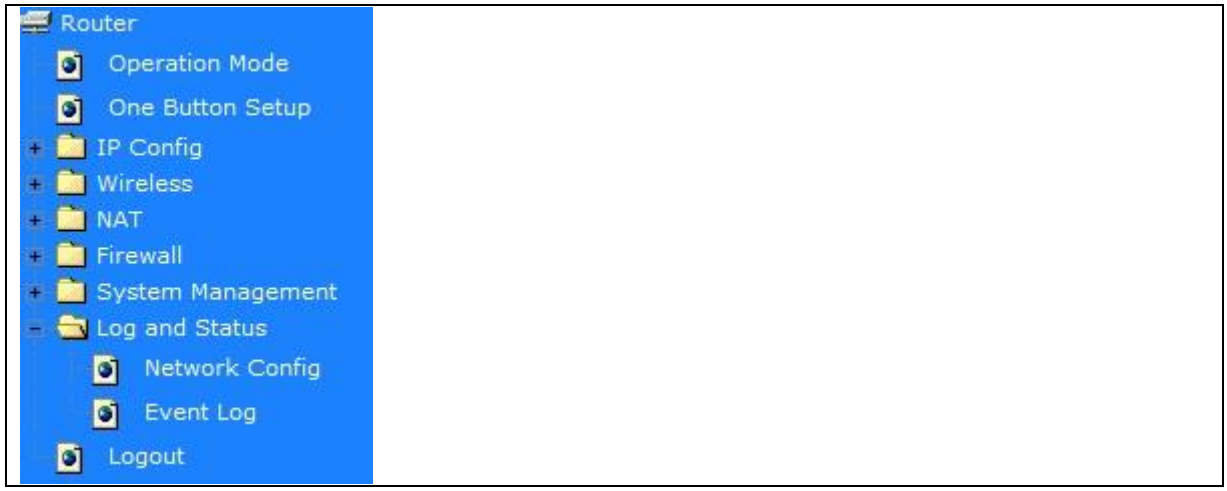
This page allows users to manually define which VPN packets may pass through the NAT firewall without being modified.



These settings are all enabled by default, simply choose disabled and click on Apply Changes if you do not want these traffics to pass the NAT firewall.

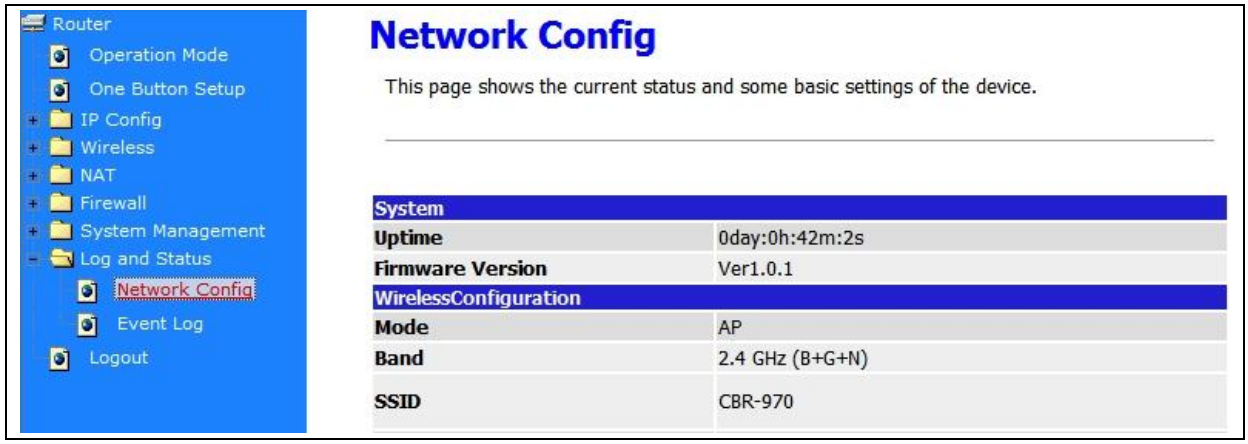
4.7 Log & Status

The category provides **Network Config** and **Event Log** status for users to know the operation status.



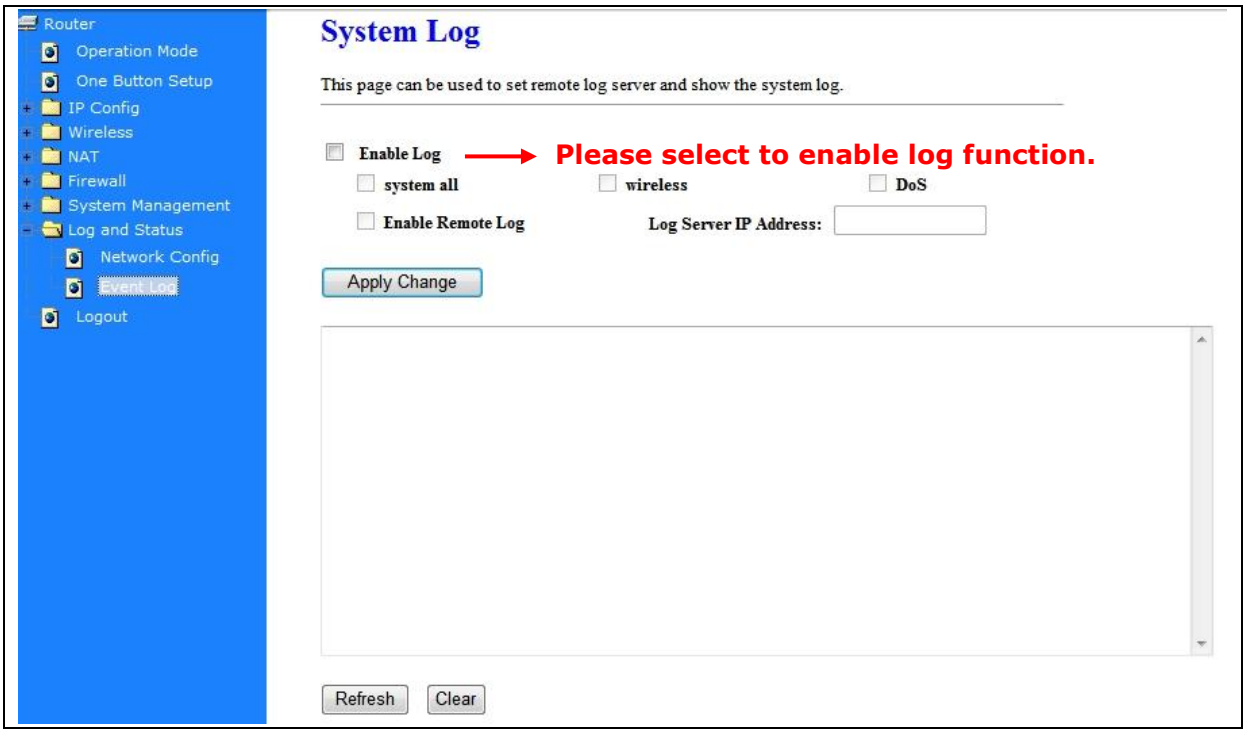
4.7.1 Network Config

Users can check the Internet status under this category, including Firmware version, Wireless setting, Connecting Time, WAN, TCP/IP …information from this page.



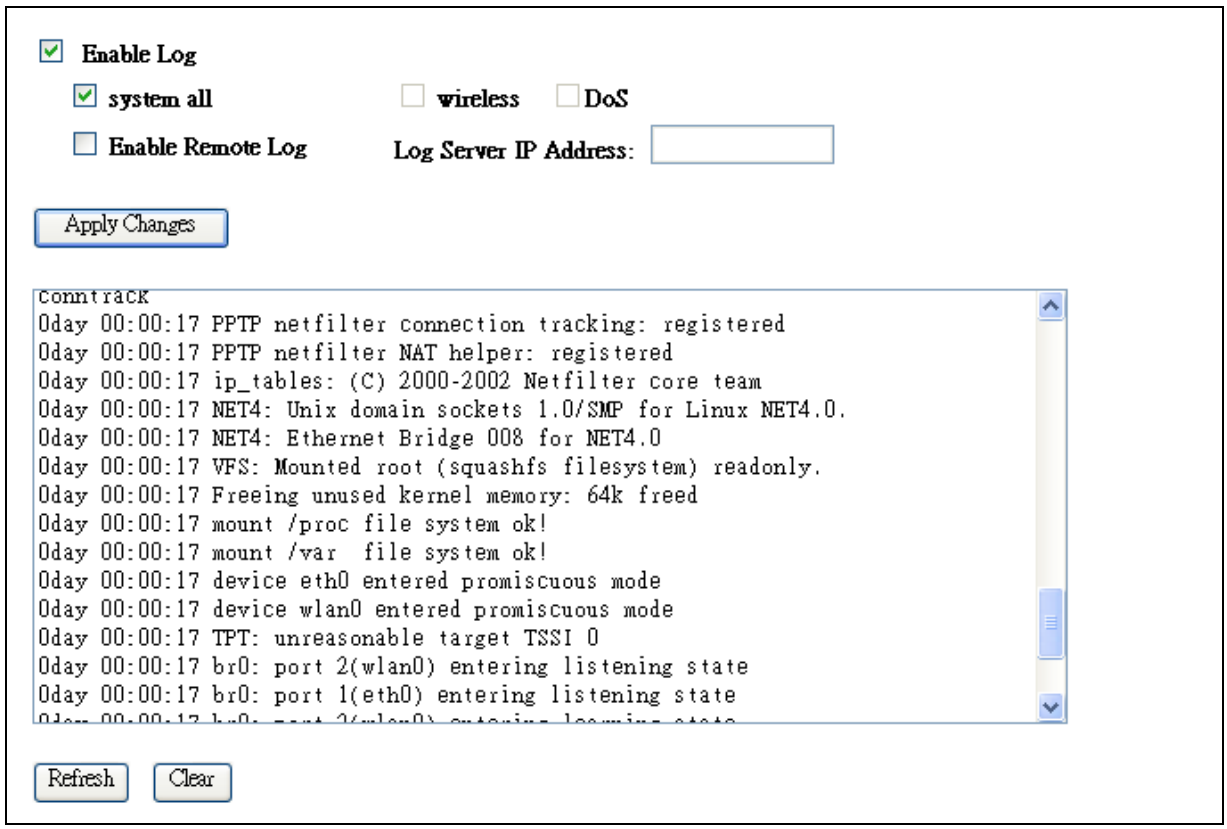
4.7.2 Event Log

You could enable the event log feature here.



Item	Description
Enable Log	You may choose to enable Event Log or not
System all, Wireless, DoS	Please select the event you want to record.
Enable Remote Log	You may choose to enable the remote event log or not.
Log Server IP Address	Please input the log server IP Address.
Apply & Cancel	Click on **Apply** button to add the settings into the list table. Click on **Cancel** button to clean the setting on this page.

*The following figure is an example when users click **Apply Changes** to record the event log.


Enable Log
system all
wireless
DoS
Enable Remote Log
Log Server IP Address:
Apply Changes
Conntrack
0day 00:00:17 PPTP netfilter connection tracking: registered
0day 00:00:17 PPTP netfilter NAT helper: registered
0day 00:00:17 ip_tables: (C) 2000-2002 Netfilter core team
0day 00:00:17 NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
0day 00:00:17 NET4: Ethernet Bridge 008 for NET4.0
0day 00:00:17 VFS: Mounted root (squashfs filesystem) readonly.
0day 00:00:17 Freeing unused kernel memory: 64k freed
0day 00:00:17 mount /proc file system ok!
0day 00:00:17 mount /var file system ok!
0day 00:00:17 device eth0 entered promiscuous mode
0day 00:00:17 device wlan0 entered promiscuous mode
0day 00:00:17 TPT: unreasonable target TSSI 0
0day 00:00:17 br0: port 2(wlan0) entering listening state
0day 00:00:17 br0: port 1(eth0) entering listening state
Refresh
Clear

4.8 Logout

This function logs out the user.

Chapter 5 AP Mode Advanced Configuration

5.1 IP Config

In this category, you can setup the IP rules under AP Mode.

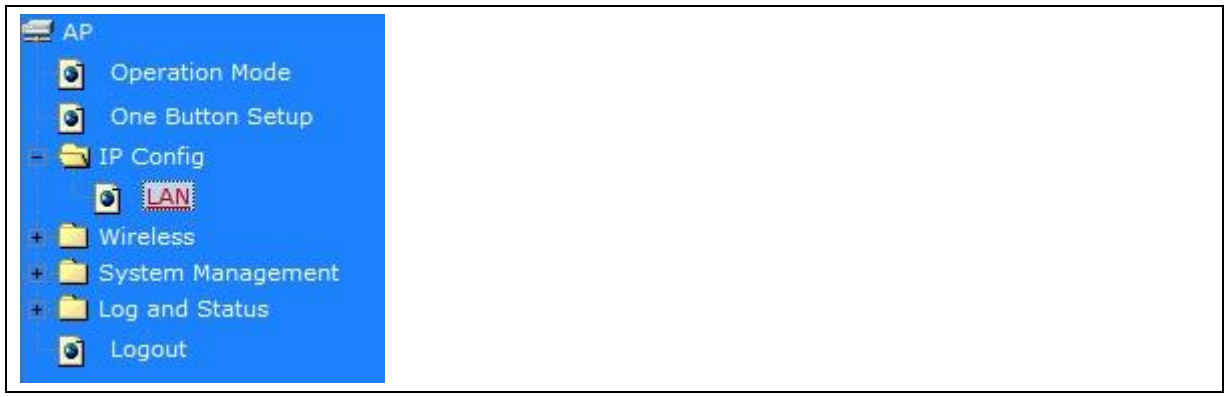
Default IP Address: 192.168.1.254

Default IP subnet mask: 255.255.255.0

WEB login User Name: admin

WEB login Password: admin

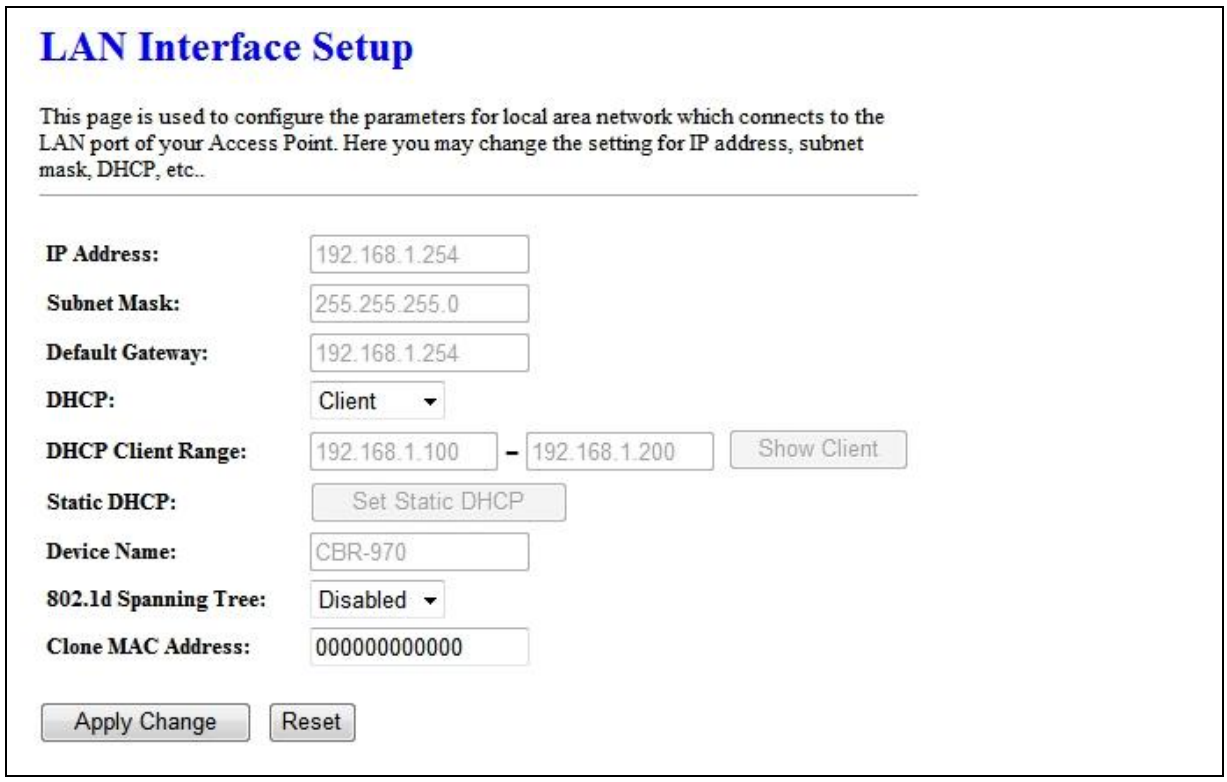
5.1.1 LAN Setup



Please click on **LAN** of **IP Config** and follow the below setting.

5.1.2 LAN Interface Setup

This page is used to configure for local area network which connects to the LAN port of your Access Point. Here users may change the setting for IP address, Subnet Mask, DHCP, etc.



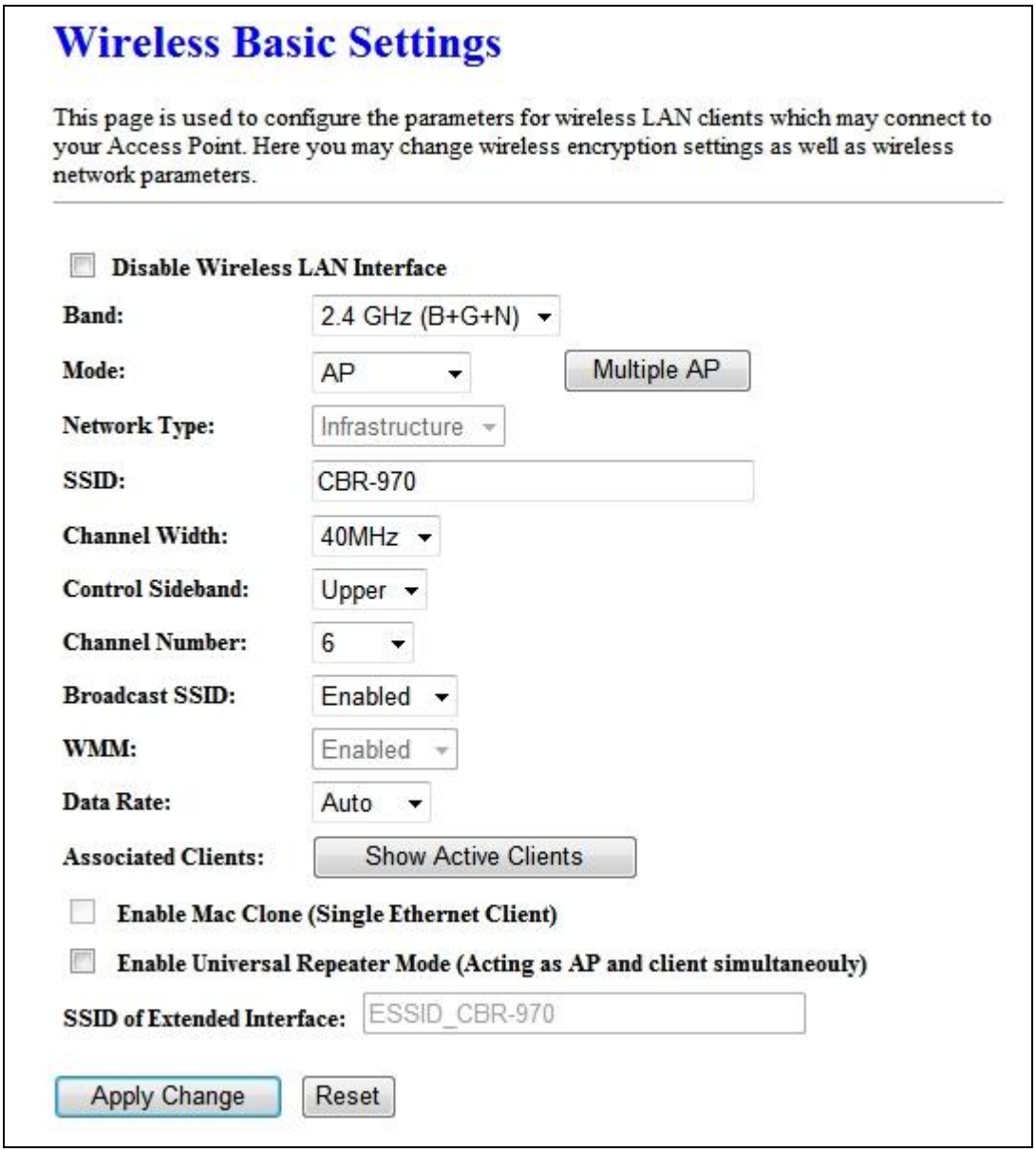
Item	Description
IP Address	The default IP address is **192.168.1.254**
Subnet Mask	Please enter the Subnet Mask address
Default Gateway	Please enter the Default Gateway address for LAN interface.
DHCP	Click to select **Disabled, Client** or **Server** in different operation mode of LAN access point.
DHCP Client Range	Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range
Static DHCP	Configures how static DHCP address are assigned to client (only available when DHCP server is enabled)
Device Name	Configures the device name of the router.
802.1d Spanning Tree	IEEE 802.1d **Spanning Tree Protocol** (**STP**) is a link layer network protocol that ensures a loop-free topology for any bridged LAN, This function is optional.
Clone MAC Address	If your ISP asks you to enter a specific MAC Address, please input the correct info at the column.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

5.2 Wireless Setup

The category includes **Basic Settings**, **Advanced Settings**, **Security**, **Access Control**, **WDS settings**, and **WPS**. Please read below for the setting instruction.

5.2.1 Wireless Basic Settings

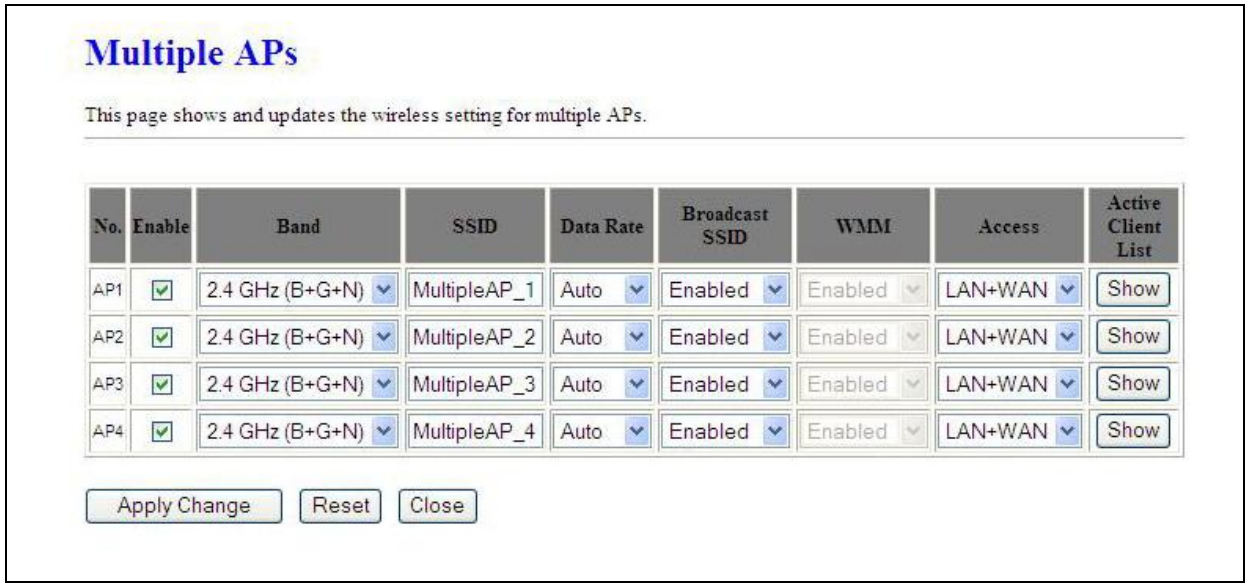
The Wireless Basic Settings include Band, Mode, SSID, Channel Number and other wireless settings.



Item	Description
Disable Wireless LAN Interface	Turn off the wireless service.
Band	Please select the frequency. It has 6 options: 2.4 GHz (B/G/N/B+G/G+N/B+G+N).
Mode	Please select the mode. It has 3 modes to select:(AP, Client, WDS, AP+WDS). **Multiple APs** provides users another 4 different SSID for connection. Users can add or limit the properties for each connection. Please check Section 5.2.1.1
SSID	Service Set identifier, the default SSID is **CNet**, users can define to any.
Channel Width	Please select the channel width, it has 2 options: 20MHZ, and 40MHZ.
Control Sideband	Enable this function will control your router use lower or upper channel.
Channel Number	Please select the channel; it has Auto, 1, 2~11 or 13 options.
Broadband SSID	User may choose to enable **Broadcast SSID** or not.
Data Rate	Please select the data transmission rate.
Associate Clients	Check the AP connectors and the Wireless connecting status.
Enable MAC Clone (Single Ethernet Client)	Clone the MAC address for ISP to identify.
SSID of Extended Interface	While linking the upper level device in wireless way, you can set SSID to give the bottom layer user search.
Apply Change & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

5.2.1.1 Multiple APs

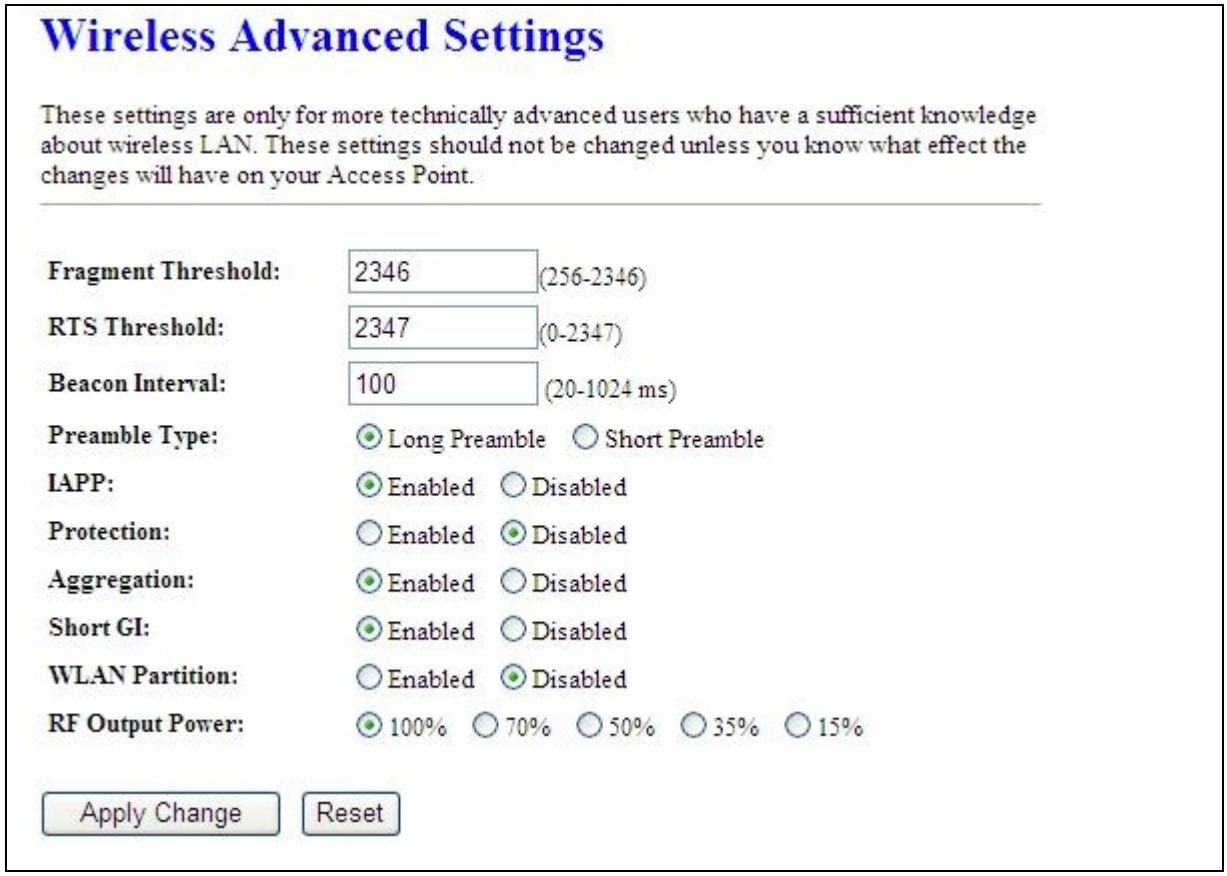
Multiple APs provides users another 4 different SSIDs for connection. Each SSID could be set with different data rate, WMM and access type.


Multiple APs
This page shows and updates the wireless setting for multiple APs.
No. Enable Band SSID Data Rate Broadcast SSID WMM Access Active Client List
AP1 2.4 GHz (B+G+N) MultipleAP_1 Auto Enabled Enabled LAN+WAN Show
AP2 2.4 GHz (B+G+N) MultipleAP_2 Auto Enabled Enabled LAN+WAN Show
AP3 2.4 GHz (B+G+N) MultipleAP_3 Auto Enabled Enabled LAN+WAN Show
AP4 2.4 GHz (B+G+N) MultipleAP_4 Auto Enabled Enabled LAN+WAN Show
Apply Change
Reset
Close

Item	Description
Enable	Enable or disable the service.
Band	Select the frequency.
SSID	Enter the SSID.
Data Rate	Select the data transmission rate.
Access	Enable this function can let clients use two access types: a. LAN+WAN: the client can access to the Internet and access in the router's GUI. b. WAN: the client can only access to the Internet.
Active Client List	Display the properties of the client which is connecting successfully.
Apply Changes	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

5.2.2 Wireless Advanced Settings

In Advanced Settings page, more 802.11 related parameters are tunable


Wireless Advanced Settings
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.
Fragment Threshold: 2346 (256-2346)
RTS Threshold: 2347 (0-2347)
Beacon Interval: 100 (20-1024 ms)
Preamble Type: Long Preamble Short Preamble
IAPP: Enabled Disabled
Protection: Enabled Disabled
Aggregation: Enabled Disabled
Short GI: Enabled Disabled
WLAN Partition: Enabled Disabled
RF Output Power: 100% 70% 50% 35% 15%
Apply Change
Reset

Item	Description
Fragment Threshold	To identify the maxima length of packet, the over length packet will be fragmentized. The allowed range is 256-2346, and default length is 2346
RTS Threshold	This value should remain at its default setting of 2347. The range is 0~2347. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the present RTS threshold size, the RTS/CTS mechanism will not be enabled. The router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. Fill the range from 0 to 2347 into this blank.
Beacon Interval	Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. The allowed setting range is 20-1024 ms.

Preamble Type	PLCP is Physical layer convergence protocol and PPDU is PLCP protocol data unit during transmission, the PSDU shall be appended to a PLCP preamble and header to create the PPDU. It has 2 options: Long Preamble and Short Preamble.
IAPP	Inter-Access Point Protocol is a recommendation that describes an optional extension to IEEE 802.11 that provides wireless access-point communications among multivendor systems.
Protection	Please select to enable wireless protection or not.
Aggregation	Enable this function will combine several packets to one and transmit it. It can reduce the problem when mass packets are transmitting.
Short GI	Users can get better wireless transmission efficiency when they enable this function.
RF Output Power	Users can adjust RF output power to get the best wireless network environment. Users can choose from 100%, 70%, 50%, 35%, and 15%.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

5.2.3 Wireless Security Setup

Here users define the security type and level of the wireless network. Selecting different methods provides different levels of security. **Please note that using any encryption may cause a significant degradation of data throughput on the wireless link**. There are five Encryption types supported: “None”, “WEP”, “WPA (TKIP)”, ”WPA2(AES)”, and “WPA2 Mixed”.

Wireless Security Setup
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.
Select SSID:
Root AP - CBR-970
Apply Change
Reset
Encryption:
Disable
802.1x Authentication:

Encryption -- WEP Key

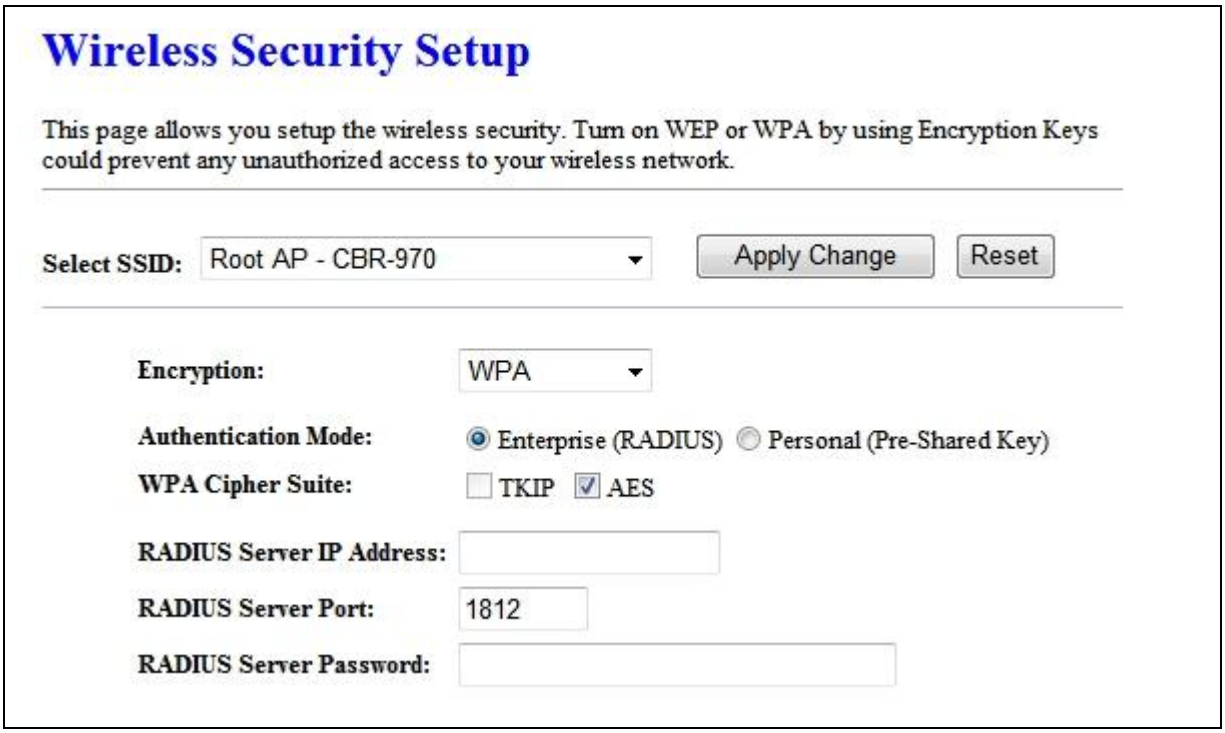
Set WEP Key: This section provides 64bit and 128bit WEP encryptions and two different shared key formats (ASCII and Hex) for wireless network.

802.1x Authentication: It is a safety system by using authentication to protect your wireless

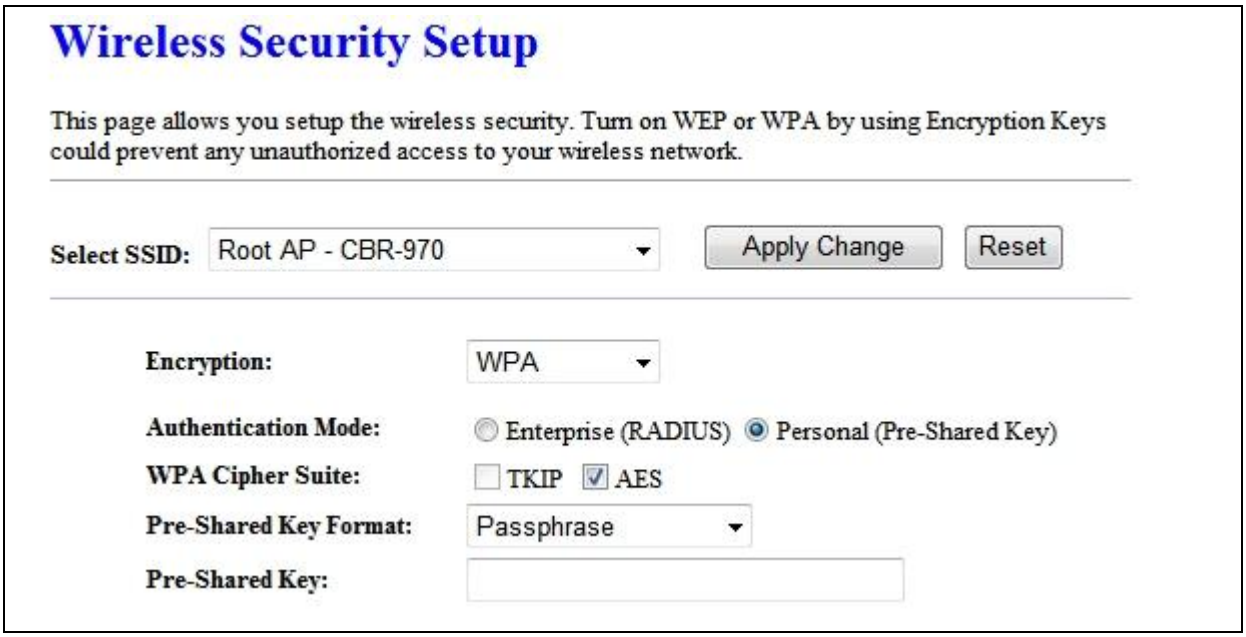
network.

Encryption – WPA (WPA, WPA2, and WPA2 Mixed), WPA Authentication Mode

- Enterprise (RADIUS): Please fill in the RADIUS server Port, IP Address, and Password



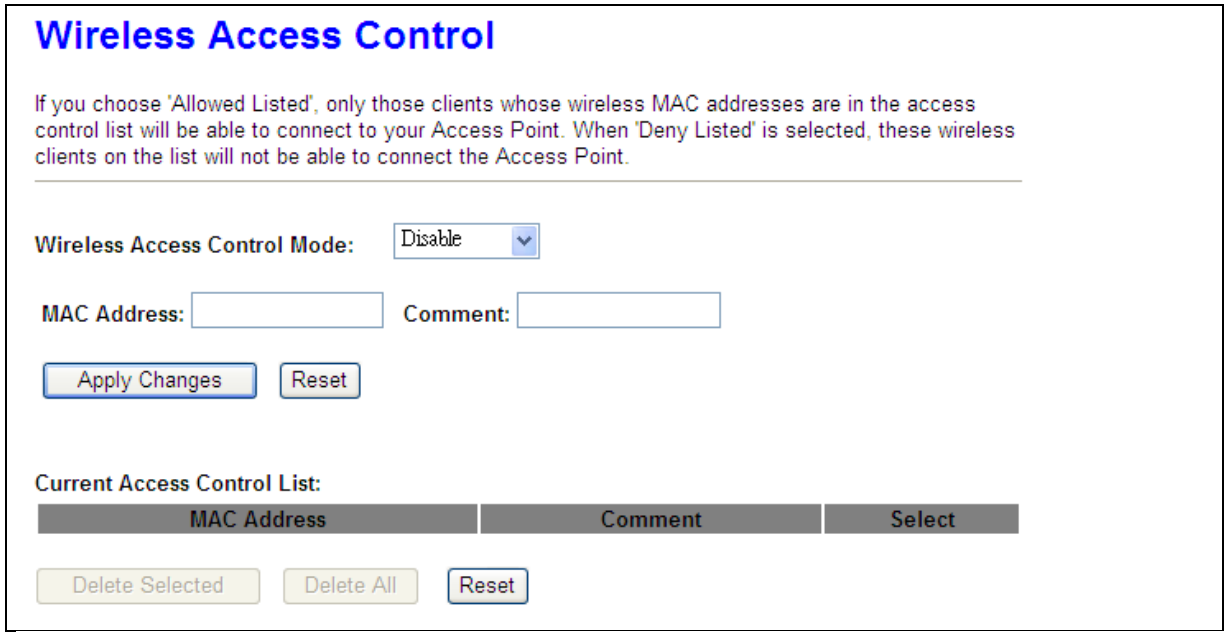
- Personal (Pre-Shared Key): Pre-Shared Key type is ASCII Code; the length is between 8 to 63 characters. If the key type is Hex, the key length is 64 characters



Apply Change & Reset: Click on **'Apply Changes'** to save setting data. Or click **'Reset'** to reset all the input data

5.2.4 Wireless Access Control

Access Control allows user to block or allow wireless clients to access this router. Users can select the access control mode, then add a new MAC address with a simple comment and click on "**Apply Changes**" to save the new addition. To delete a MAC address, select its corresponding checkbox under the **Select** column and click on "**Delete** Selected" button.


Wireless Access Control
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.
Wireless Access Control Mode:
Disable
MAC Address:
Comment:
Apply Changes
Reset
Current Access Control List:
MAC Address
Comment
Select
Delete Selected
Delete All
Reset

Take the wireless card as the example.

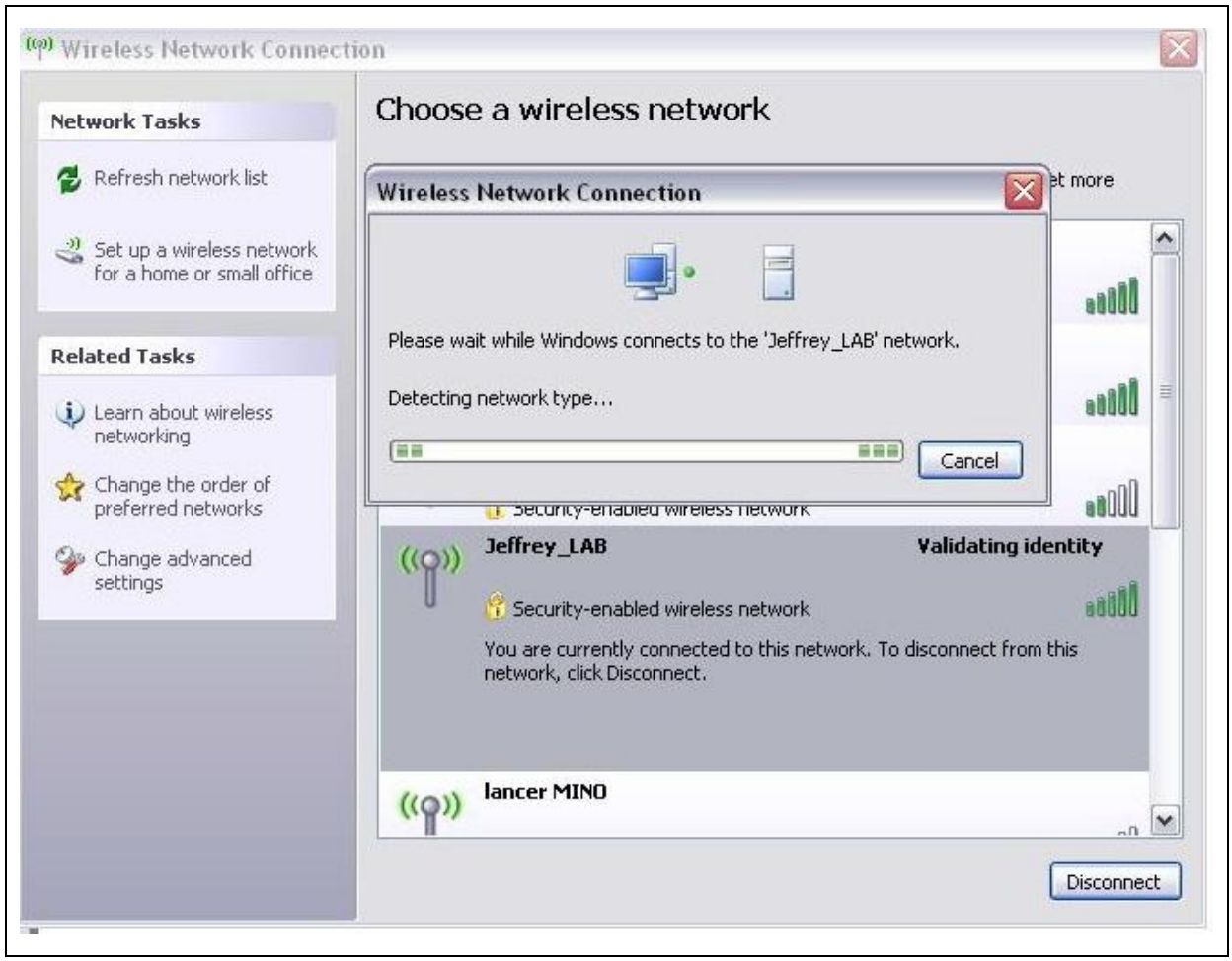
(1) Here is the example. Please select **Deny Listed** in **Wireless Access Control Mode** first, and then fill in the MAC address what you plan to block in the MAC Address field. Click **Apply Changes** to save the setting.

Wireless Access Control
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.
Wireless Access Control Mode:
Deny Listed
MAC Address:
0018F8638A54
Comment:
Apply Change
Reset
Current Access Control List:
MAC Address
Comment
Select
Delete Selected
Delete All
Reset

(2) The MAC address what you set will be displayed on the **Current Access Control List**.

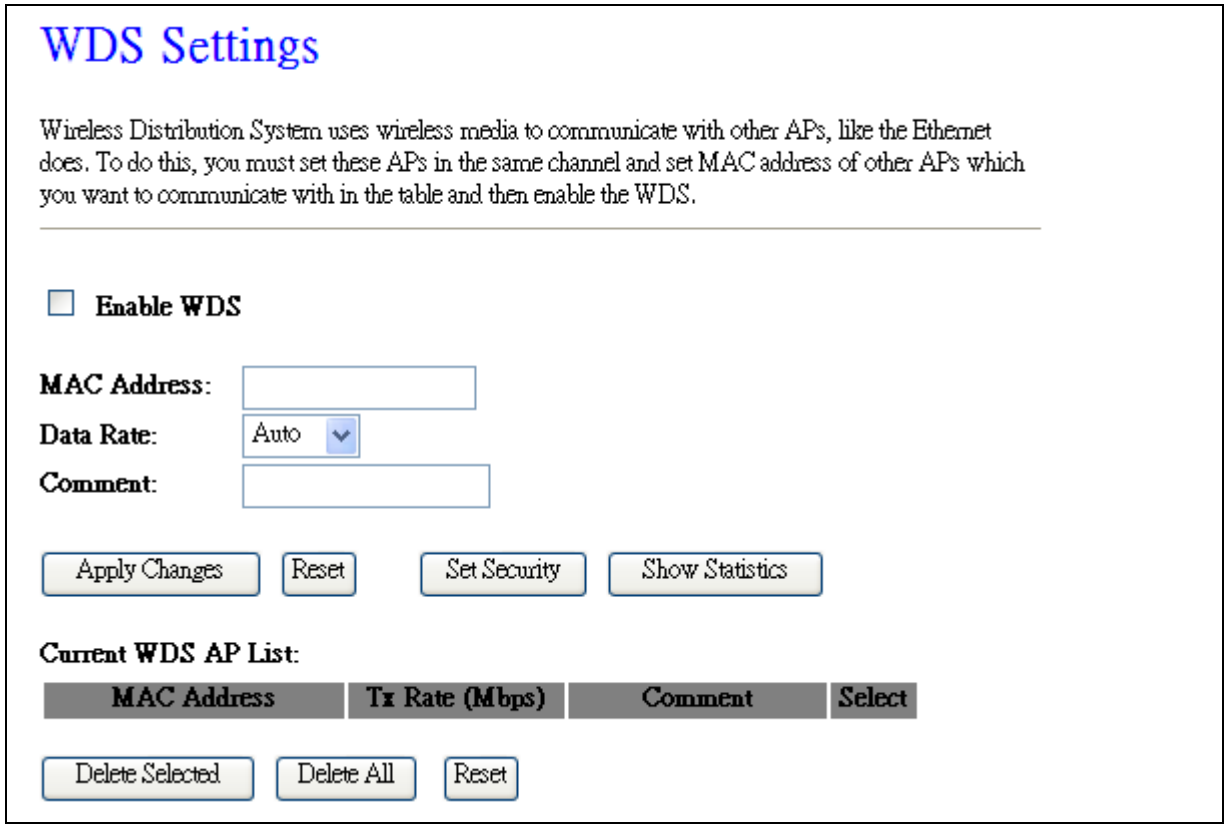
Wireless Access Control
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.
Wireless Access Control Mode:
Deny Listed
MAC Address:
Comment:
Apply Change
Reset
Current Access Control List:
MAC Address
Comment
Select
00:18:f8:63:8a:54
Delete Selected
Delete All
Reset

(3) The wireless client will be denied by the wireless router.

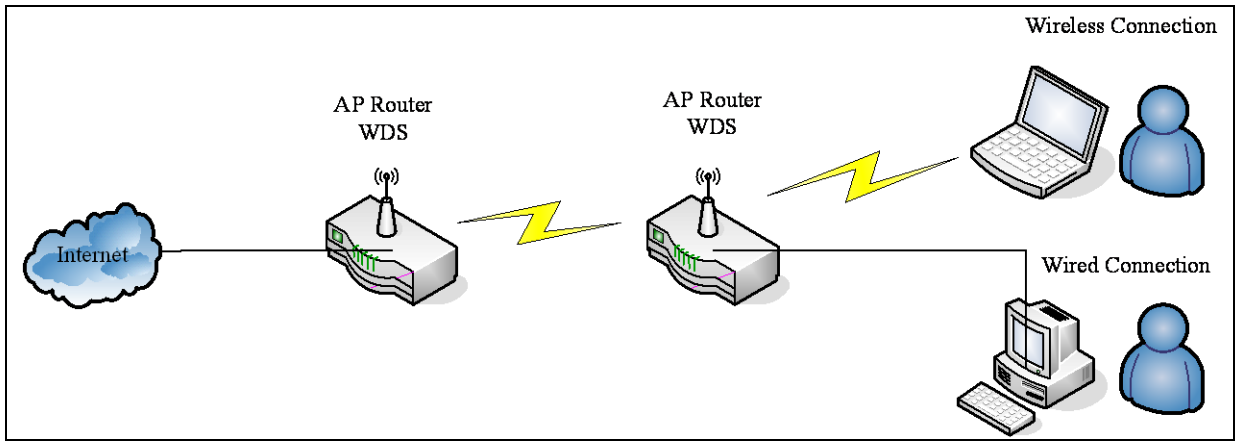

Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Wireless Network Connection
Please wait while Windows connects to the 'Jeffrey_LAB' network.
Detecting network type...
Cancel
Jeffrey_LAB
Validating identity
Security-enabled wireless network
You are currently connected to this network. To disconnect from this network, click Disconnect.
lancer MINO
Disconnect

5.2.5 WDS Settings

When selected in the Basic Settings page and enabled here, Wireless Distribution System (WDS) enables the router to be used as a wireless bridge. Two Wireless-G Routers in bridge mode can communicate with each other through their wireless interfaces. To accomplish this, all wireless routers should be set to the same channel and the MAC address of other AP / Routers should be entered in the table.

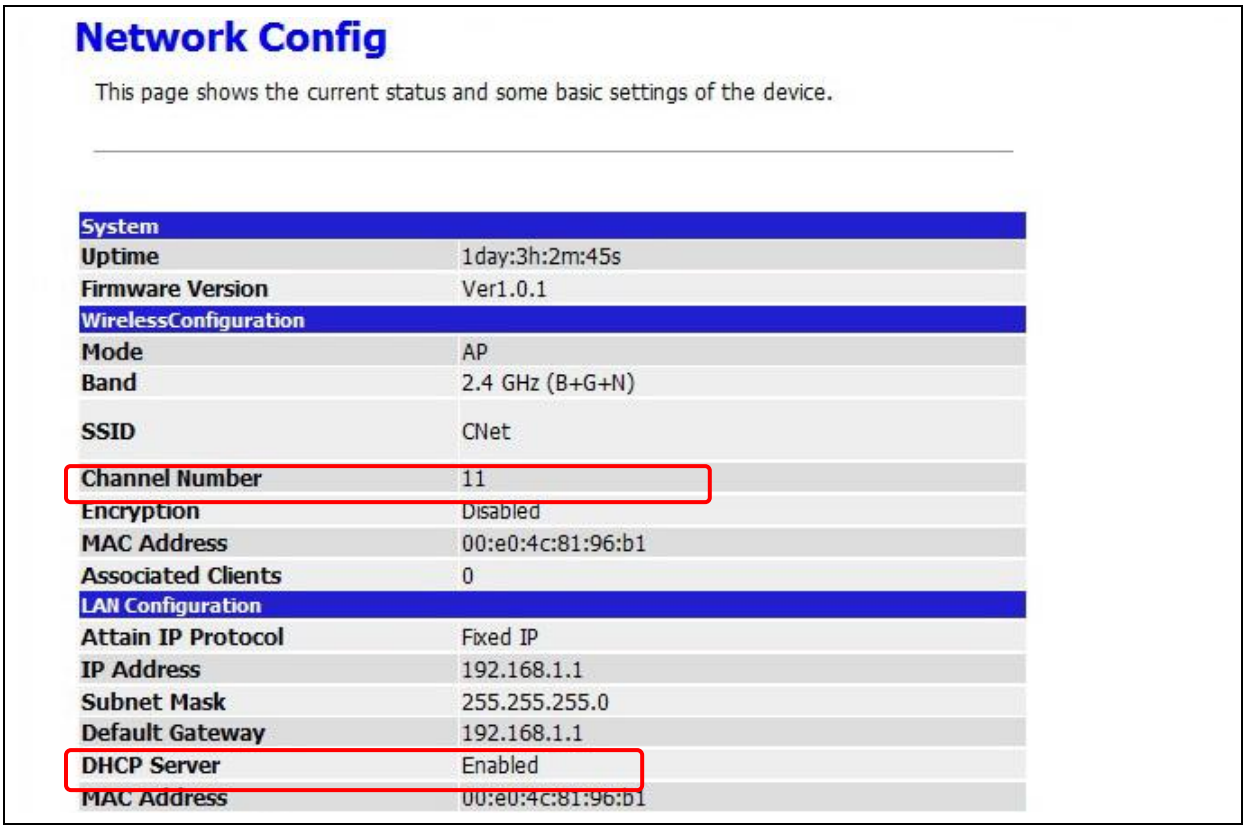

WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.
Enable WDS
MAC Address:
Data Rate:
Auto
Comment:
Apply Changes
Reset
Set Security
Show Statistics
Current WDS AP List:
MAC Address
Tx Rate (Mbps)
Comment
Select
Delete Selected
Delete All
Reset

The WDS explanation as the following picture.

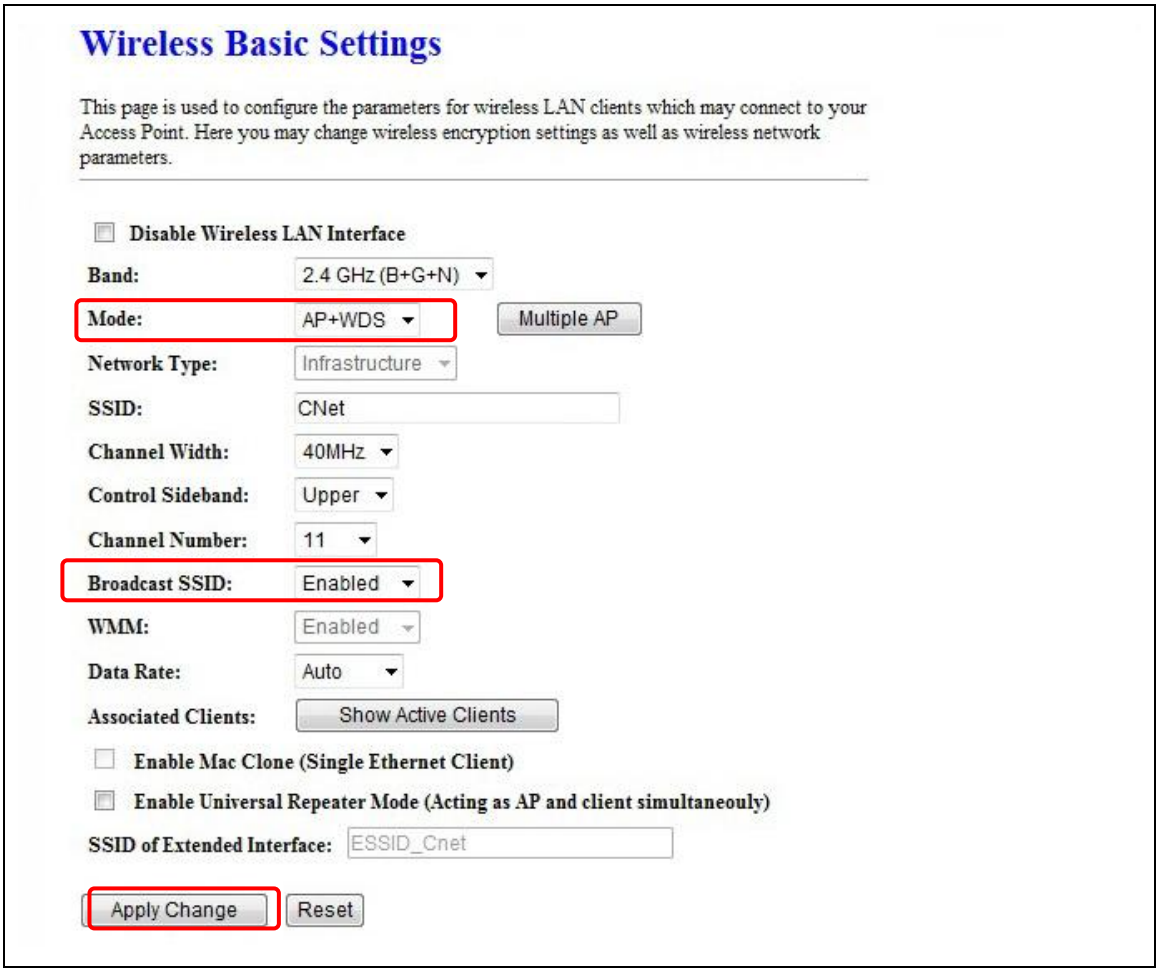


*Please follow the below instructions to setup the WDS connection.

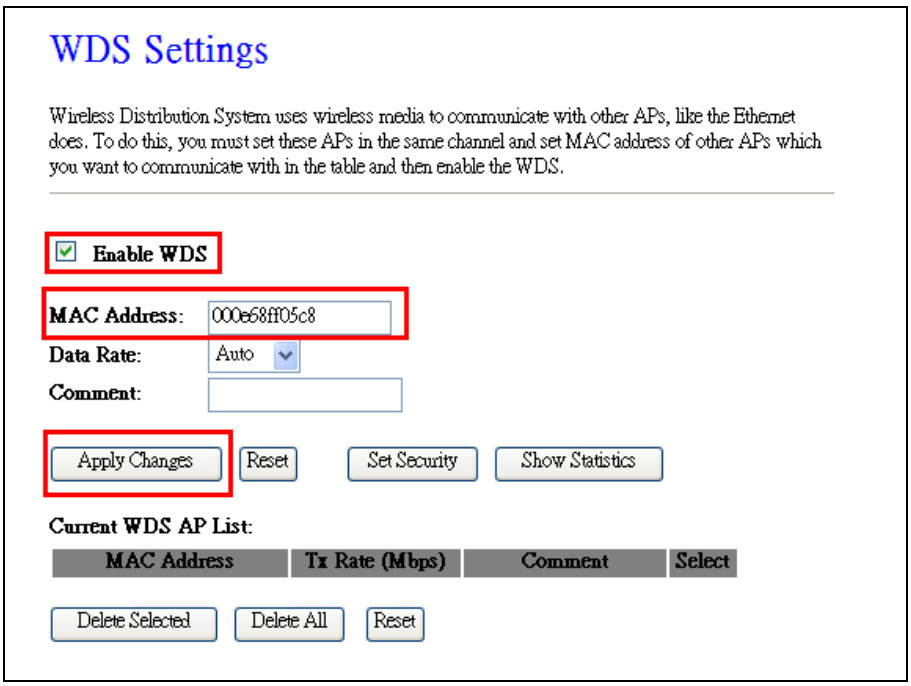
(1) Please check the MAC address and Channel number from the upper lever device.



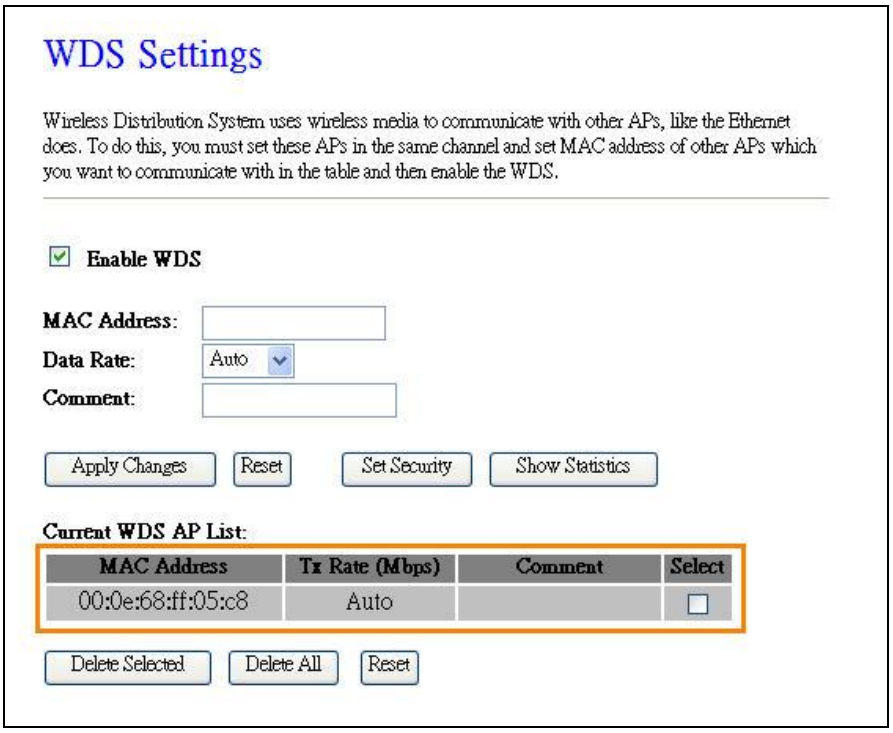
(2) Set the connection mode to “AP+WDS” from “Wireless Basic Setting”, and then select the channel number(in this example is “11”). Click **Apply Changes** to save the setting.



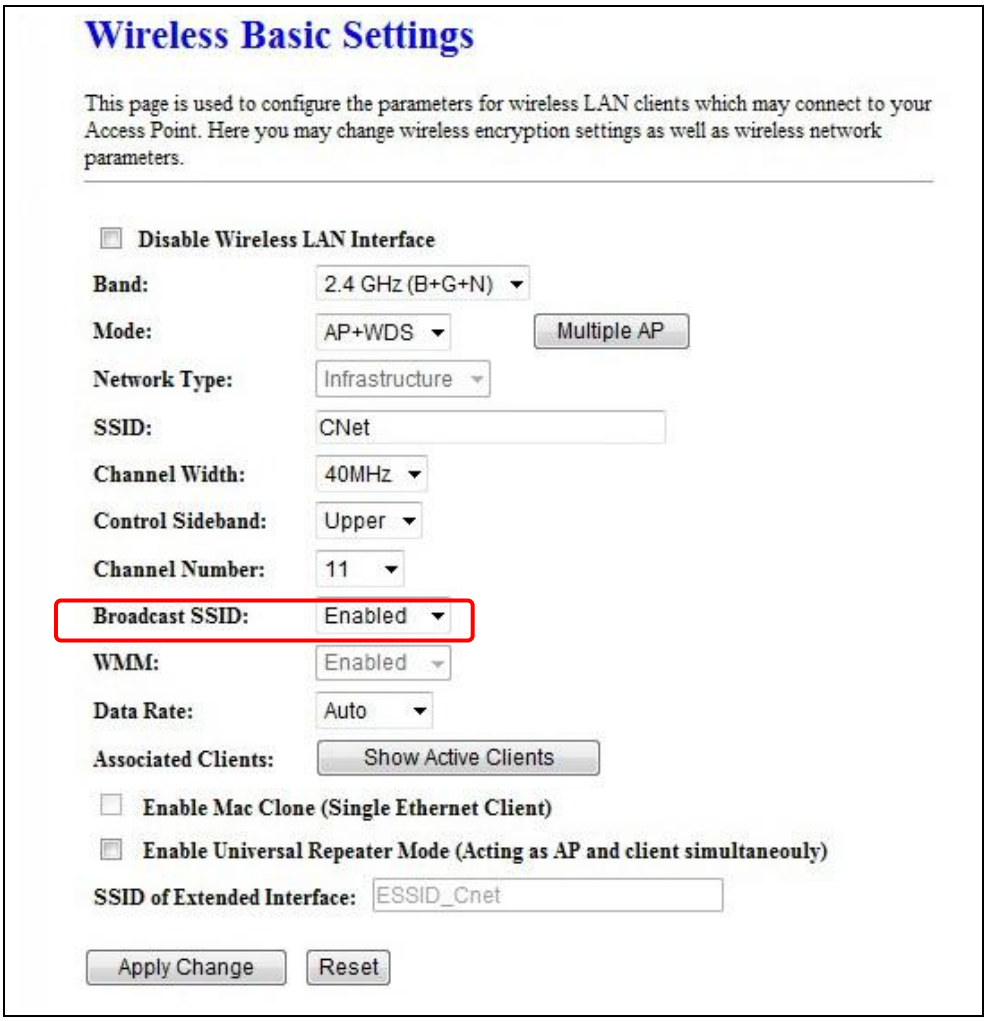
(3) Enable WDS function from the page – "WDS Setting", and then fill in the upper level device MAC address. Click **Apply Changes** to save the setting data.


WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.
Enable WDS
MAC Address:
000e68ff05c8
Data Rate:
Auto
Comment:
Apply Changes
Reset
Set Security
Show Statistics
Current WDS AP List:
MAC Address
Tx Rate (Mbps)
Comment
Select
Delete Selected
Delete All
Reset

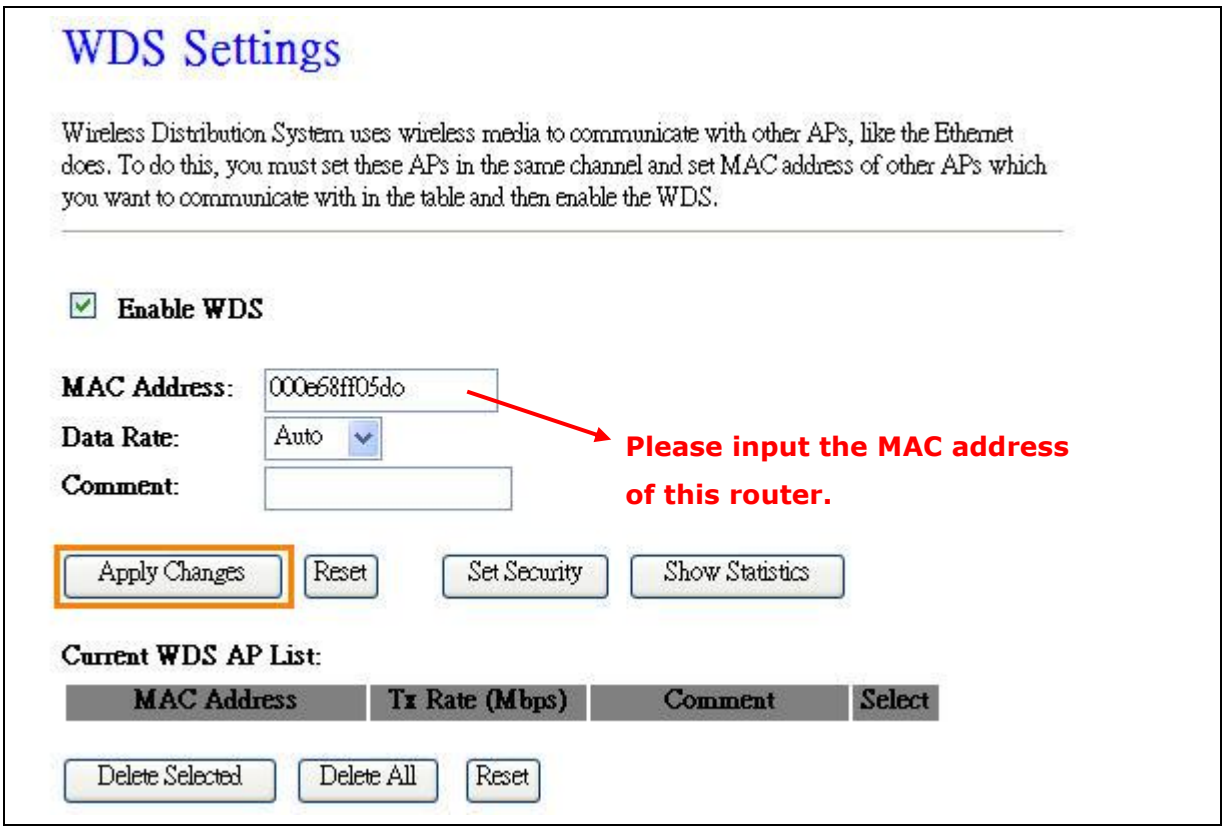
(4) The WDS AP List will show the WDS device MAC address after reboot.


WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.
Enable WDS
MAC Address:
Data Rate:
Auto
Comment:
Apply Changes
Reset
Set Security
Show Statistics
Current WDS AP List:
MAC Address
Tx Rate (Mbps)
Comment
Select
00:0e:68:ff:05:c8
Auto
Delete Selected
Delete All
Reset

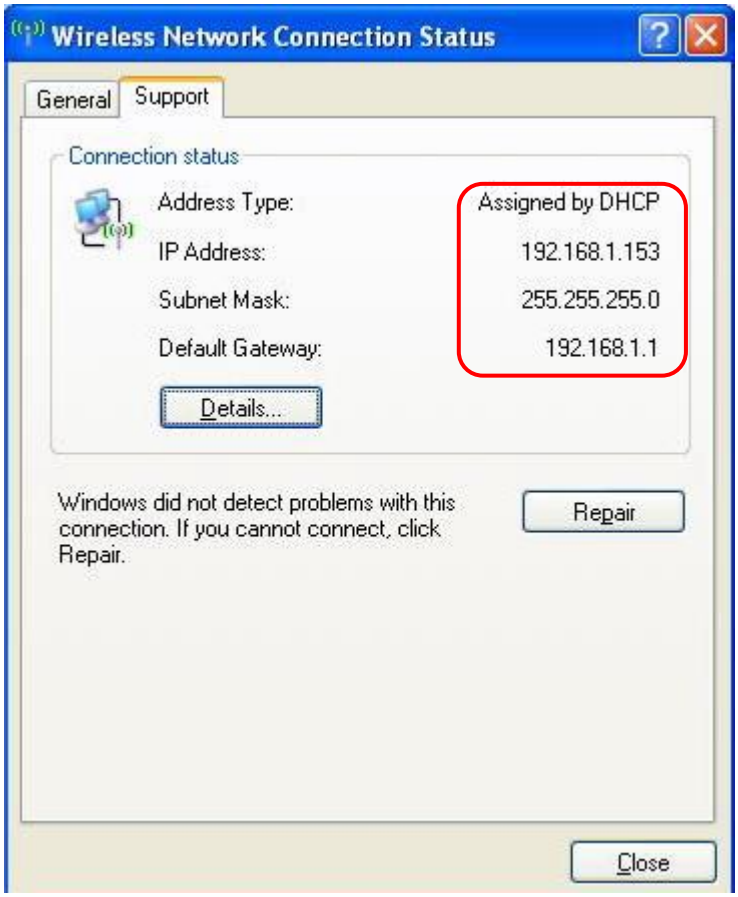
(5) Set “Broadcast SSID” to disable from page “Wireless Basic Setting”.



(6) Go to the upper level device WDS setting page and fill in the MAC address


WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.
Enable WDS
MAC Address:
000e68ff05do
Data Rate:
Auto
Comment:
Please input the MAC address of this router.
Apply Changes
Reset
Set Security
Show Statistics
Current WDS AP List:
MAC Address
Tx Rate (Mbps)
Comment
Select
Delete Selected
Delete All
Reset

(7) You will receive an IP address from the upper lever device.



5.2.6 WPS

Please refer to Chapter **4.2.6** for detailed WPS configuration methods.

5.3 System Management

It has 6 sections: Change Password, Firmware Upgrade, Profiles Save, Time Zone Setting, UPnP Setting, and Language Setting. It is easy and helpful for users making more detailed settings.

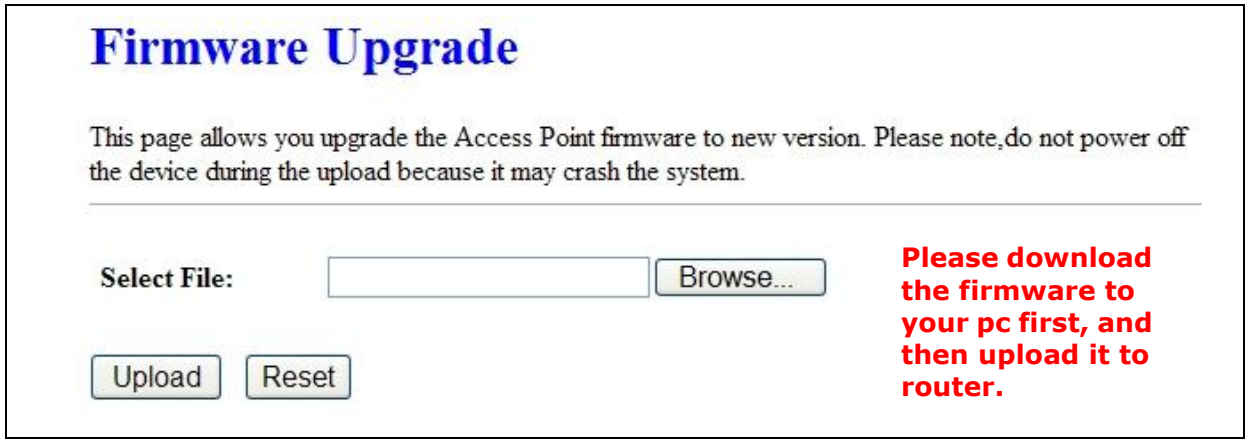
5.3.1 Change Password

Users can set or change user name and password used for accessing the web management interface in this section.

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

5.3.2 Firmware Upgrade

This function can upgrade the firmware of the router. There is certain risk while doing firmware upgrading. Firmware upgrade is not recommended unless the significant faulty is found and published on official website. If you feel the router has unusual behaviors and is not caused by the ISP and environment. You can check the website (http://www.cnet.com.tw) to see if there is any later version of firmware. Download the firmware to your computer, click **Browser** and point to the new firmware file. Click **Upload** to upgrade the firmware. You can't make any move unless the machine reboot completely.

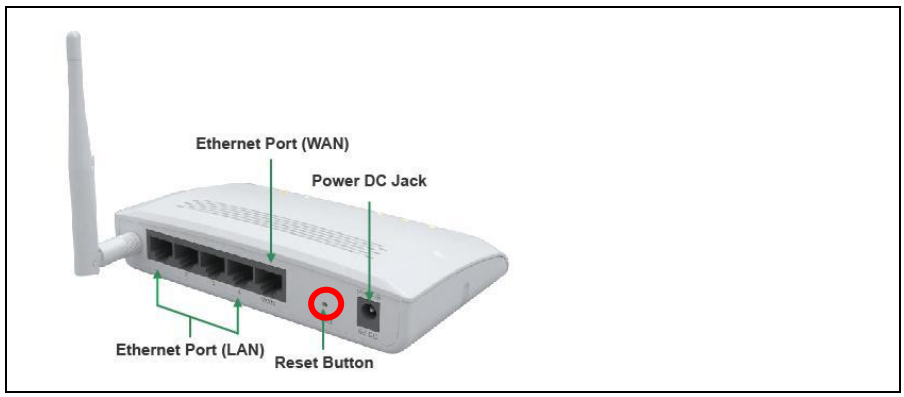

Firmware Upgrade
This page allows you upgrade the Access Point firmware to new version. Please note,do not power off the device during the upload because it may crash the system.
Select File:
Browse...
Upload
Reset
Please download the firmware to your pc first, and then upload it to router.

Caution: To prevent that firmware upgrading is interrupted by other wireless signals and causes failure. We recommend users to use wired connection during upgrading.

Caution: The firmware upgrade will not remove your previous settings.

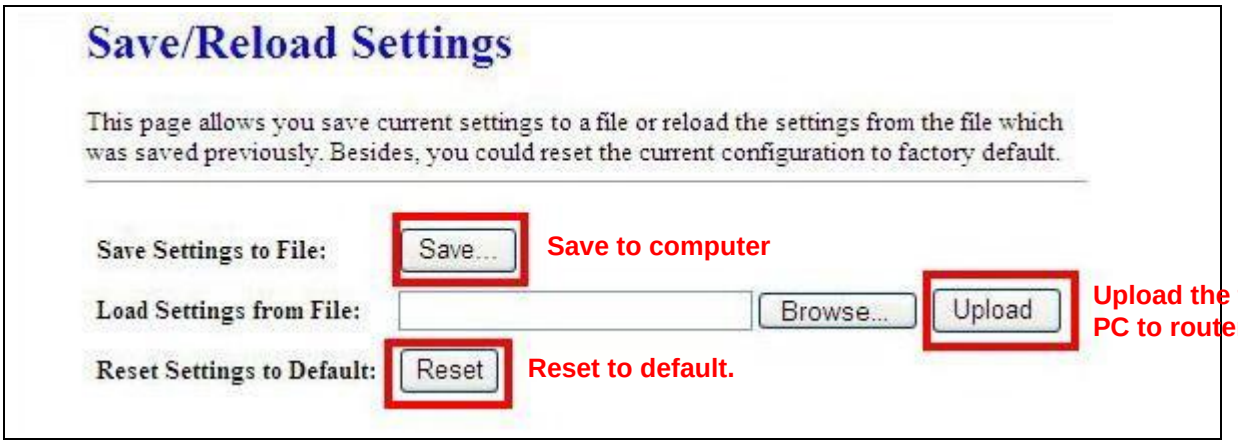
* Reset button:

On the front of this router, there is a reset button. If you cannot login the administrator page by forgetting your password; or the router has problem you can't solve. You can push the reset button for 10 seconds with a stick. The router will reboot and all settings will be restored to factory default settings. If the problem still exists, you can visit our web site to see if there is any firmware for download to solve the problem.



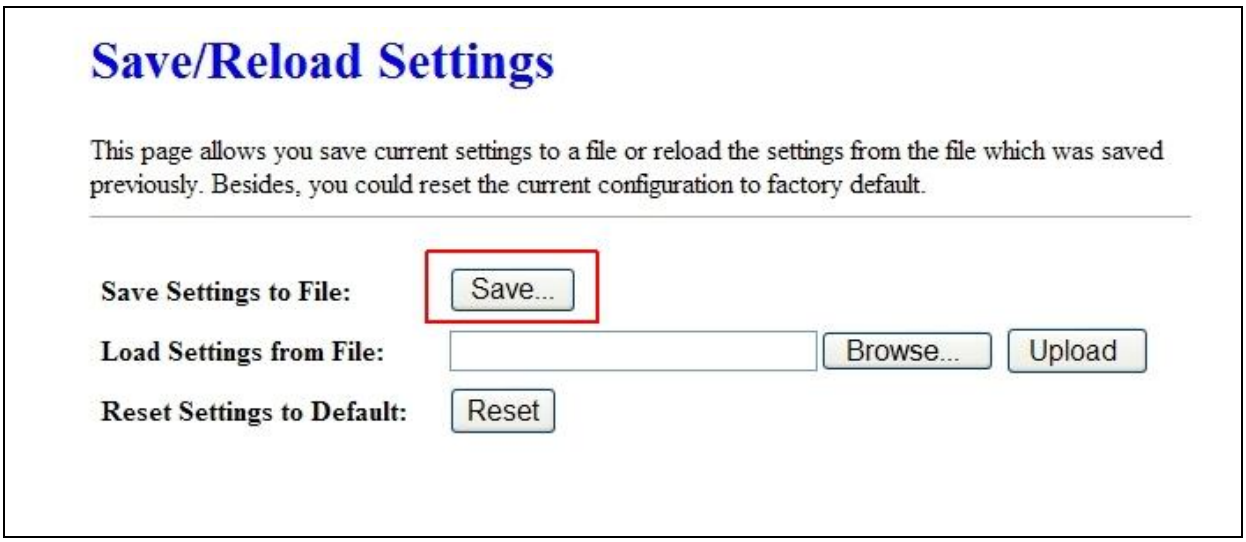
5.3.1 Profile Save

Users can create a backup file that contains current router settings. This backup file can be used to restore router settings. This is especially useful in the event you need to reset the router to its default settings.

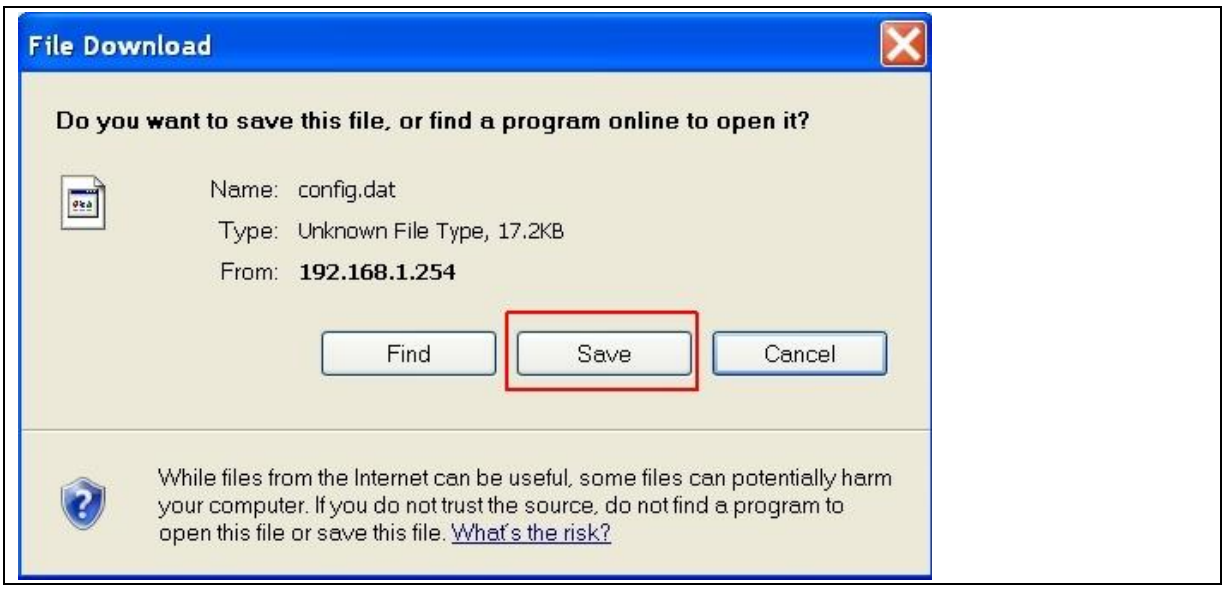

Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Save to computer
Load Settings from File:
Browse...
Upload
Upload the file from PC to router
Reset Settings to Default:
Reset
Reset to default.

a. Save Configuration

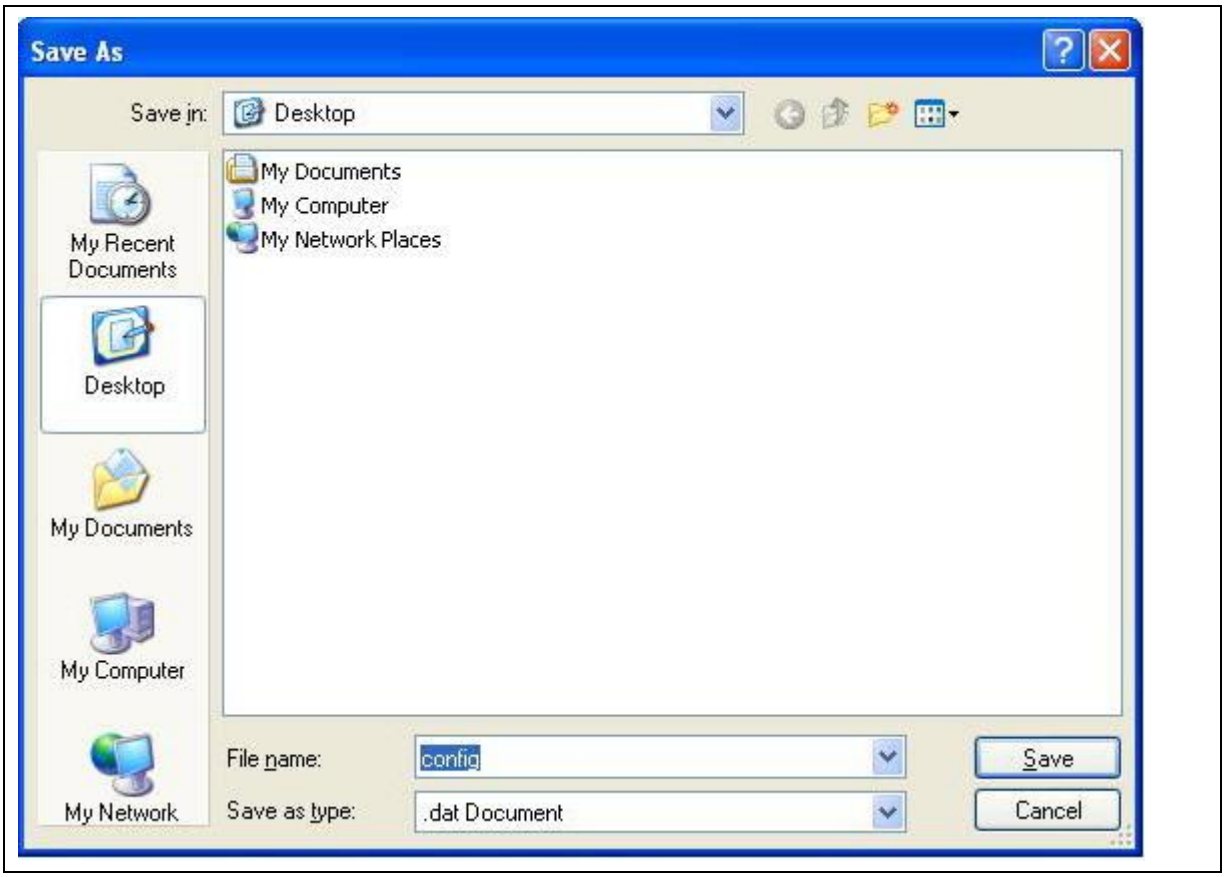
(1) Click **Save**


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Browse...
Upload
Reset Settings to Default:
Reset

(2) Please click “**Save**” to save the configuration to your computer.

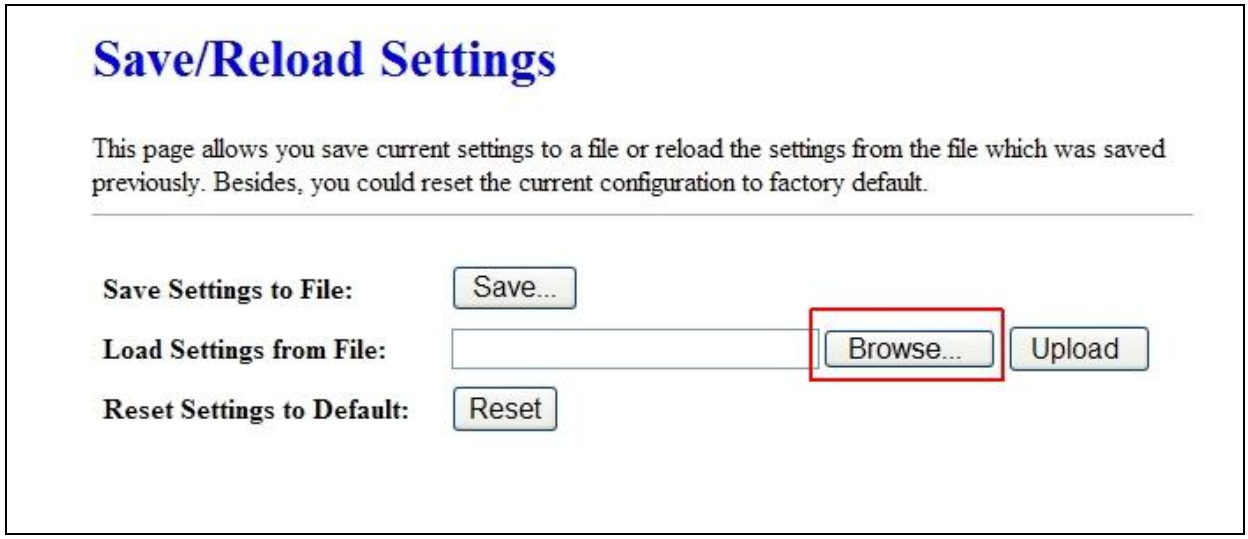

File Download
Do you want to save this file, or find a program online to open it?
Name: config.dat
Type: Unknown File Type, 17.2KB
From: 192.168.1.254
Find
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

(3) Select the location which you want to save file, then click **Save.**

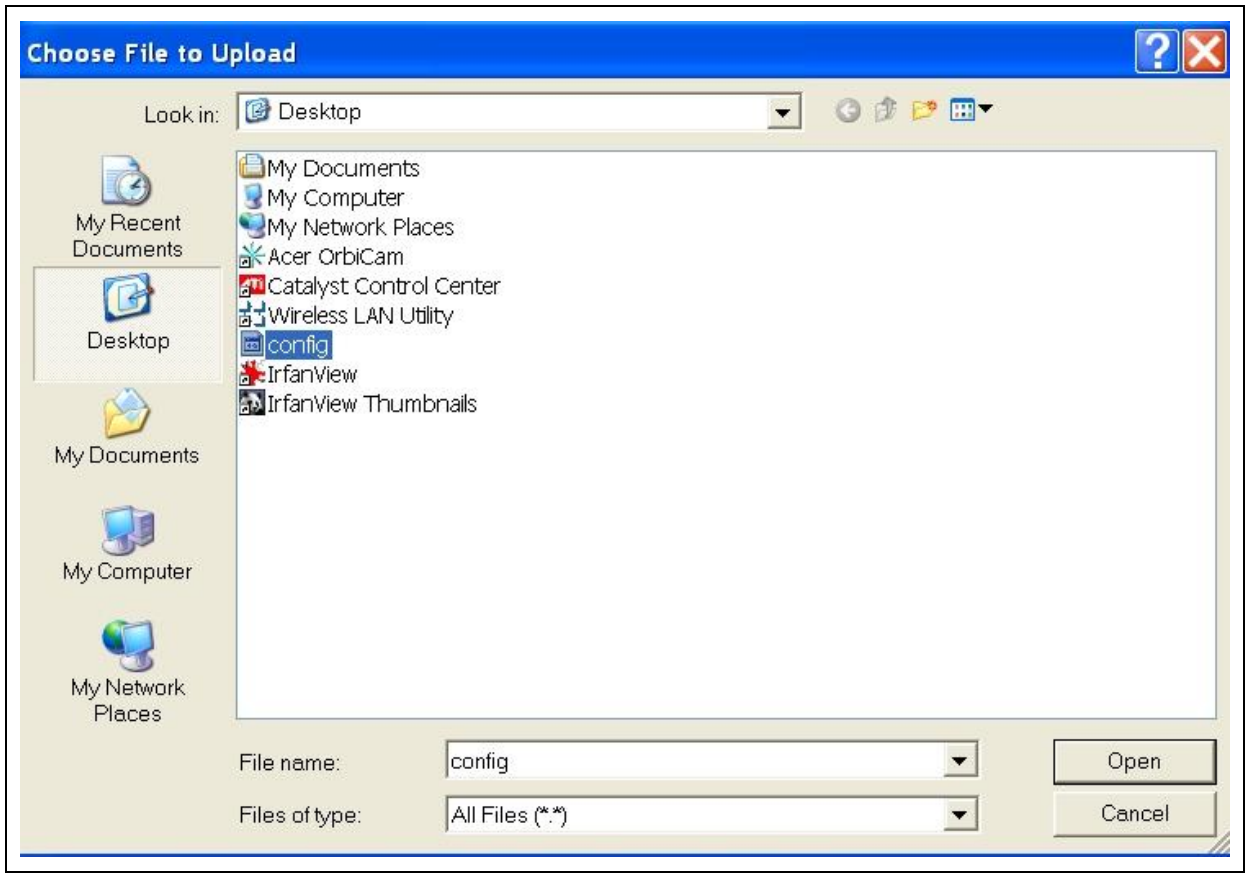


b. Load configuration file

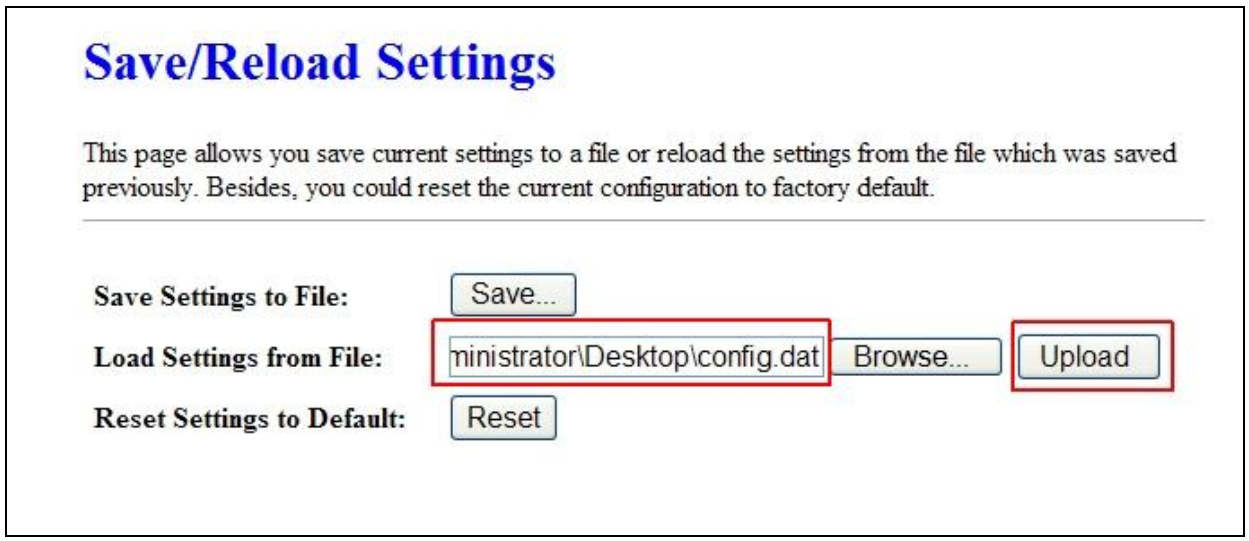
(1) Click **Browser**


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Browse...
Upload
Reset Settings to Default:
Reset

(2) Select configuration file then click **Open**



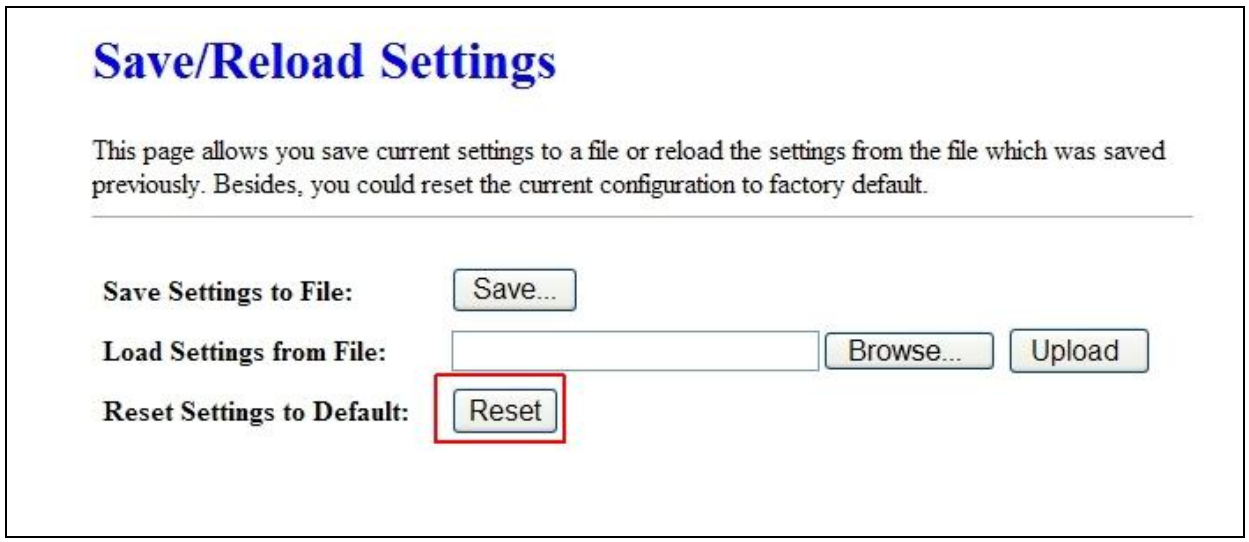
(3) Click **Upload** to upload configuration file to CBR-970/971.


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
ministrator\Desktop\config.dat
Browse...
Upload
Reset Settings to Default:
Reset

(4) After 90 seconds, CBR-970/971 will reboot automatically.

(C) Reload factory default setting

1. Please click **Reset**

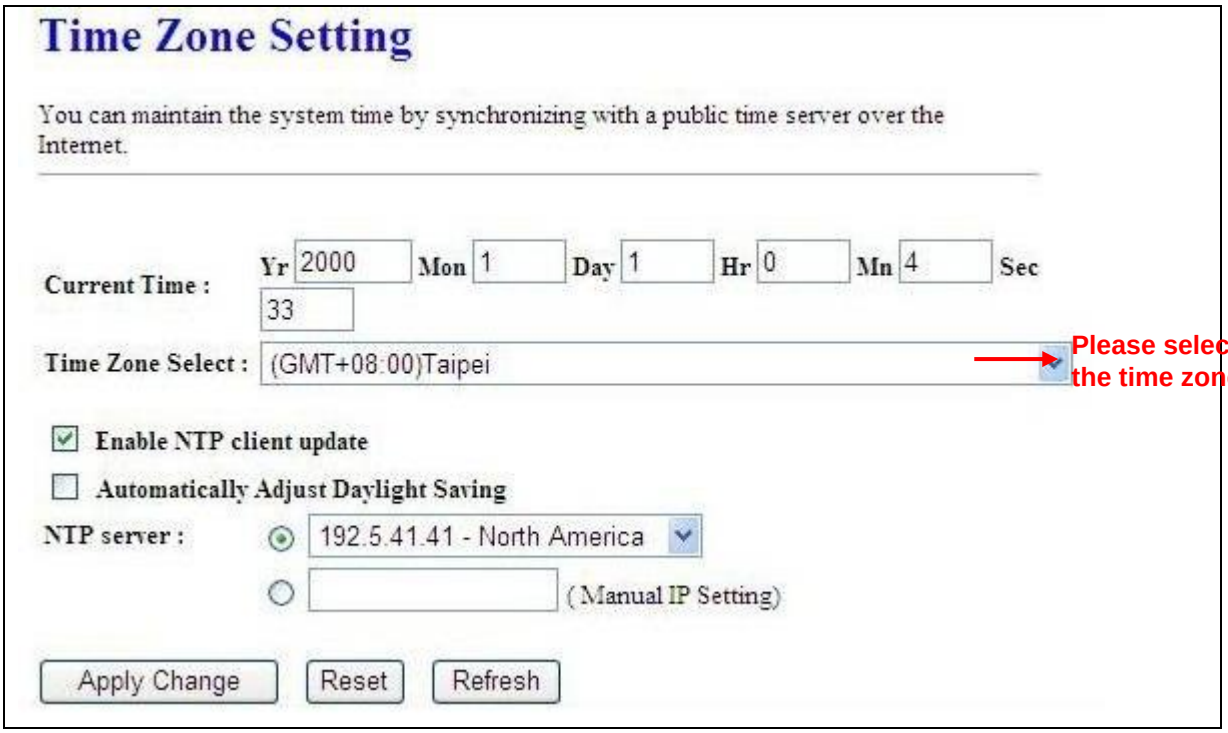

Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Browse...
Upload
Reset Settings to Default:
Reset

(2) Please click **OK** to start reload factory default setting to CBR-970/971.

(3) After 90 seconds, CBR-970/971 will reboot automatically.

5.3.2 Time Zone Setting

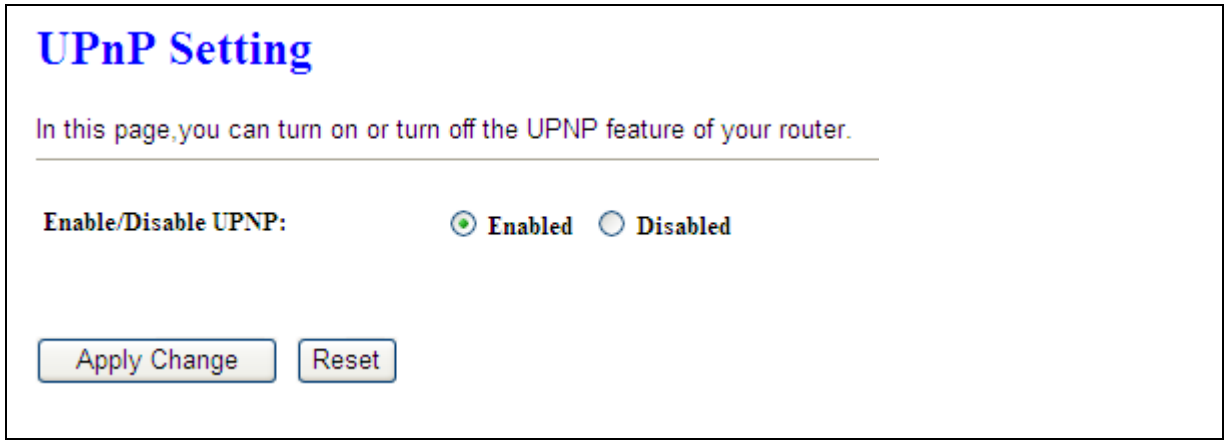
Users can synchronize the local clock on the router to an available NTP server (optional). To complete this setting, enable NTP client update and select the correct Time Zone.


Time Zone Setting
You can maintain the system time by synchronizing with a public time server over the Internet.
Current Time :
Yr 2000 Mon 1 Day 1 Hr 0 Mn 4 Sec 33
Time Zone Select :
(GMT+08:00)Taipei
Please select the time zone
Enable NTP client update
Automatically Adjust Daylight Saving
NTP server :
192.5.41.41 - North America
(Manual IP Setting)
Apply Change
Reset
Refresh

Item	Description
Current Time	Users can input the time manually.
Time Zone Select	Please select the time zone.
Enable NTP client update	Please select to enable NTP client update or not.
Automatically Adjust Daylight Saving	Please select to enable **Automatically Adjust Daylight Saving** or not.
NTP Server	Please select the NTP server from the pull-down list, or you can enter the NTP server IP address manually.
Apply Changes & Reset & Refresh	Please click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data. Or you may click on **Refresh** to update the system time on the screen.

5.3.3 UPnP Setting

Universal Plug and Play (**UPnP**) is a standard of networking protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. CBR-970/971 supports UPnP function, and can cooperate with other UPnP devices. When you activate UPnP, please click **My Network Places**. Users will see an **Internet Gateway Device** icon. By click the icon, users can enter the GUI of the router. If you do not wish to use UPnP, you can disable it.

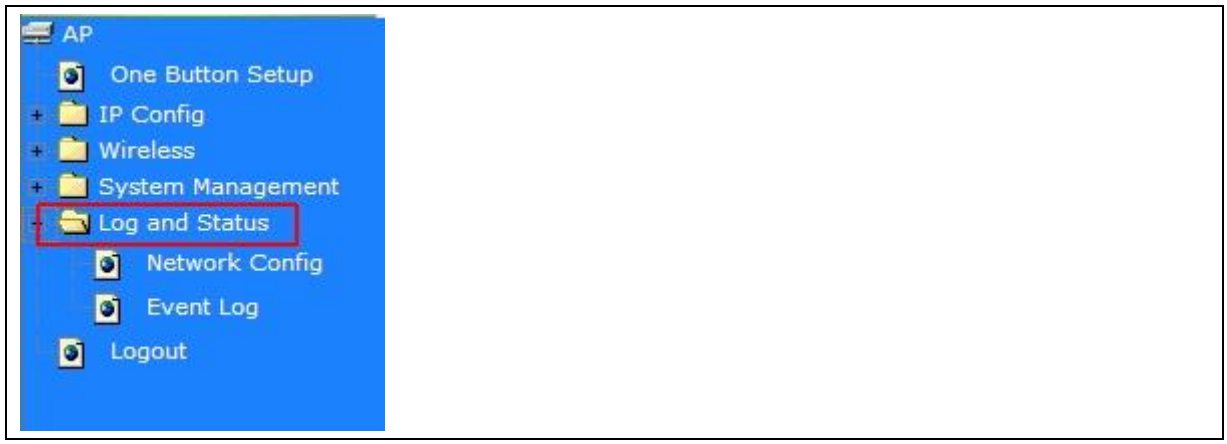


*Enable/Disable UPnP

Select to enable or disable this function.

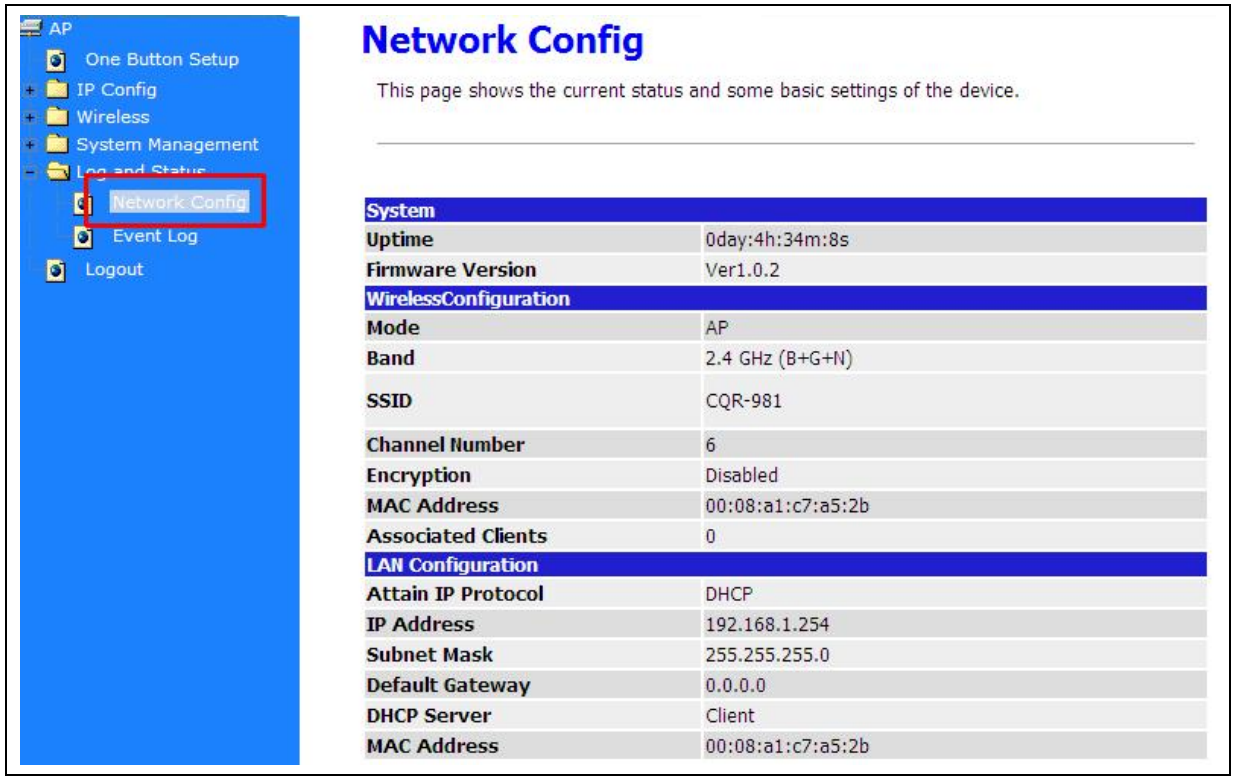
5.4 Log & Status

The category provides **Network Config** and **Event Log** status for users to know the operation status.



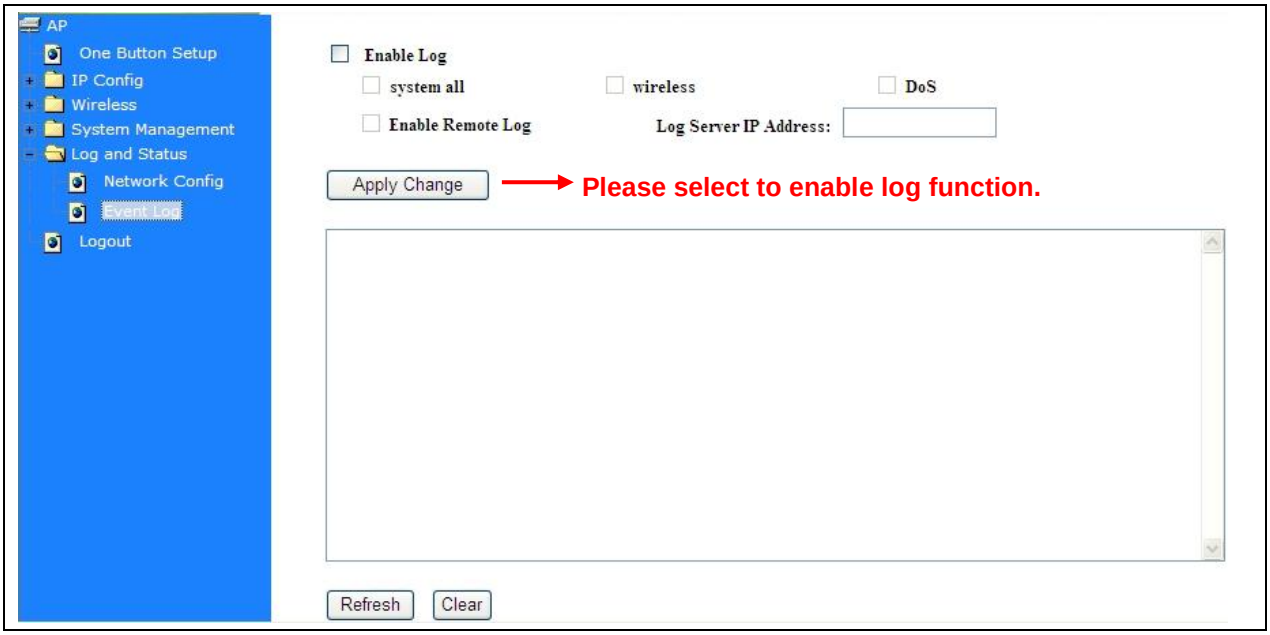
5.4.1 Network Config

Users can check the Internet status under this category, including Firmware version, Wireless setting, Connecting Time, WAN, TCP/IP …information.



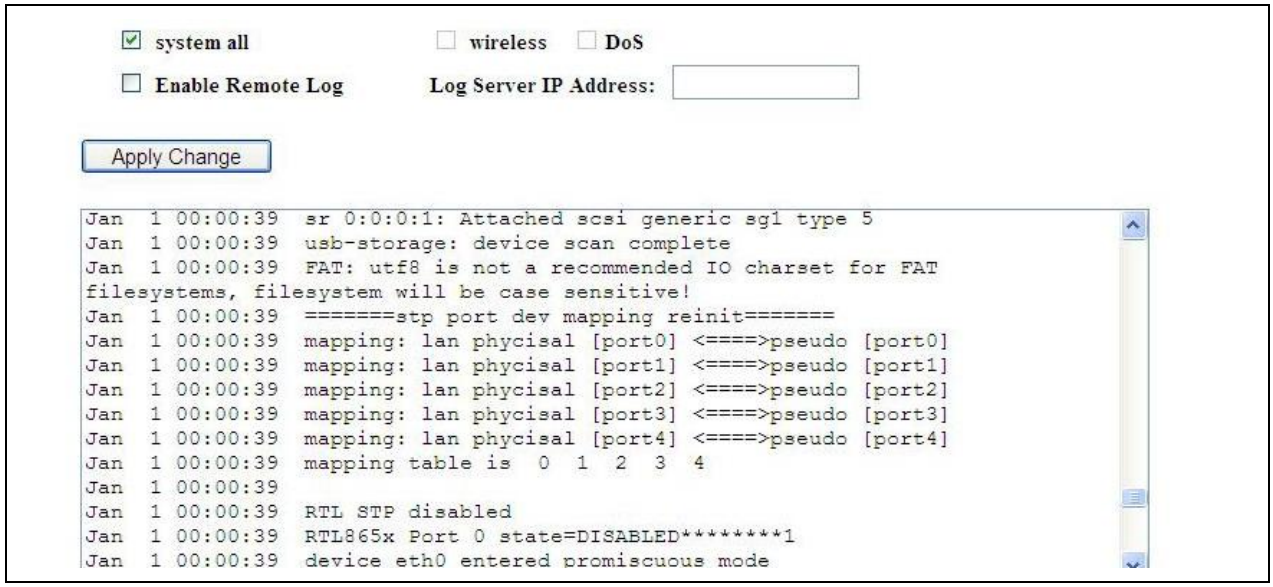
5.4.2 Event Log

You may enable the event log feature here.



Item	Description
Enable Log	You may choose to enable Event Log or not.
System all, Wireless, & DoS	Please select the event you want to record.
Enable Remote Log	You may choose to enable the remote event log or not.
Log Server IP Address	Please input the log server IP Address.
Apply Changes & Refresh & Clear	Click on **Apply Changes** to save the setting data. Click on **Refresh** to renew the system time, or on **Clear** to clear all the record.

* The following figure is an example when users click **Apply Changes** to record the event log.


system all
wireless
DoS
Enable Remote Log
Log Server IP Address:
Apply Change
Jan 1 00:00:39 sr 0:0:0:1: Attached scsi generic sg1 type 5
Jan 1 00:00:39 usb-storage: device scan complete
Jan 1 00:00:39 FAT: utf8 is not a recommended IO charset for FAT
filesystems, filesystem will be case sensitive!
Jan 1 00:00:39 =======stp port dev mapping reinit=======
Jan 1 00:00:39 mapping: lan phycisal [port0] <====>pseudo [port0]
Jan 1 00:00:39 mapping: lan phycisal [port1] <====>pseudo [port1]
Jan 1 00:00:39 mapping: lan phycisal [port2] <====>pseudo [port2]
Jan 1 00:00:39 mapping: lan phycisal [port3] <====>pseudo [port3]
Jan 1 00:00:39 mapping: lan phycisal [port4] <====>pseudo [port4]
Jan 1 00:00:39 mapping table is 0 1 2 3 4
Jan 1 00:00:39
Jan 1 00:00:39 RTL STP disabled
Jan 1 00:00:39 RTL865x Port 0 state=DISABLED********1
Jan 1 00:00:39 device eth0 entered promiscuous mode

5.5 Logout

This function logs out the user.

Chapter 6 Advanced Configuration for Wi-Fi AP Mode

6.1 IP Config

In this category, you can setup the IP rules under WiFi-AP Mode.

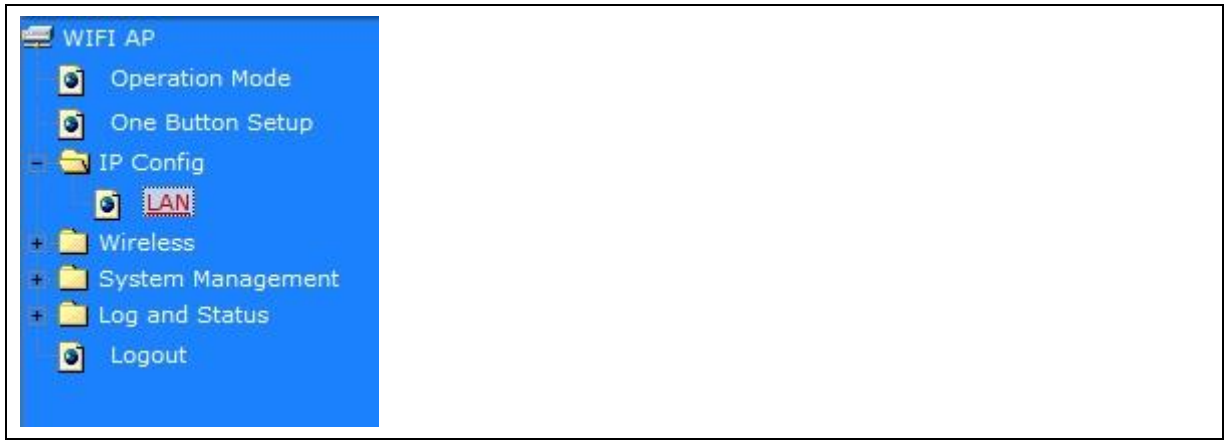
Default IP Address: 192.168.1.254

Default IP subnet mask: 255.255.255.0

WEB login User Name: admin

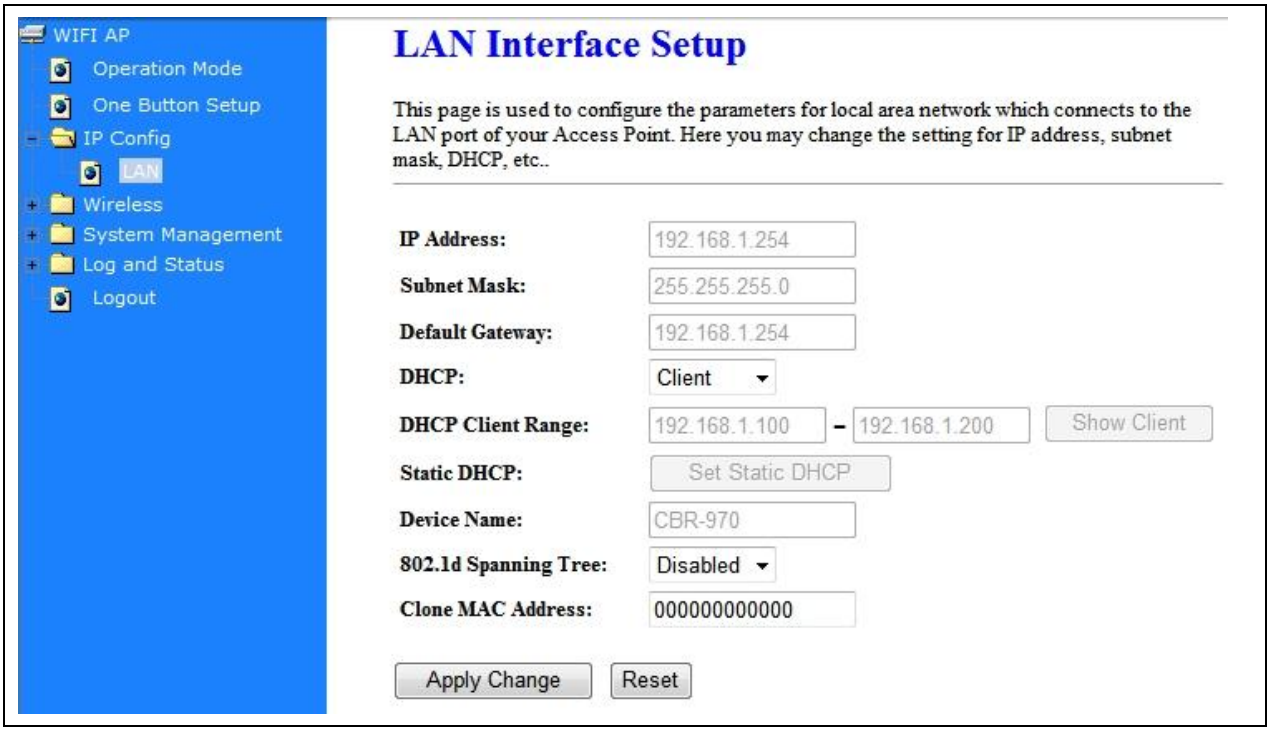
WEB login Password: admin

6.1.1 IP Config -- LAN



6.1.2 LAN Interface Setup

This page is used to configure for local area network which connects to the LAN port of your Access Point. Here users may change the setting for IP address, Subnet Mask, DHCP, etc.



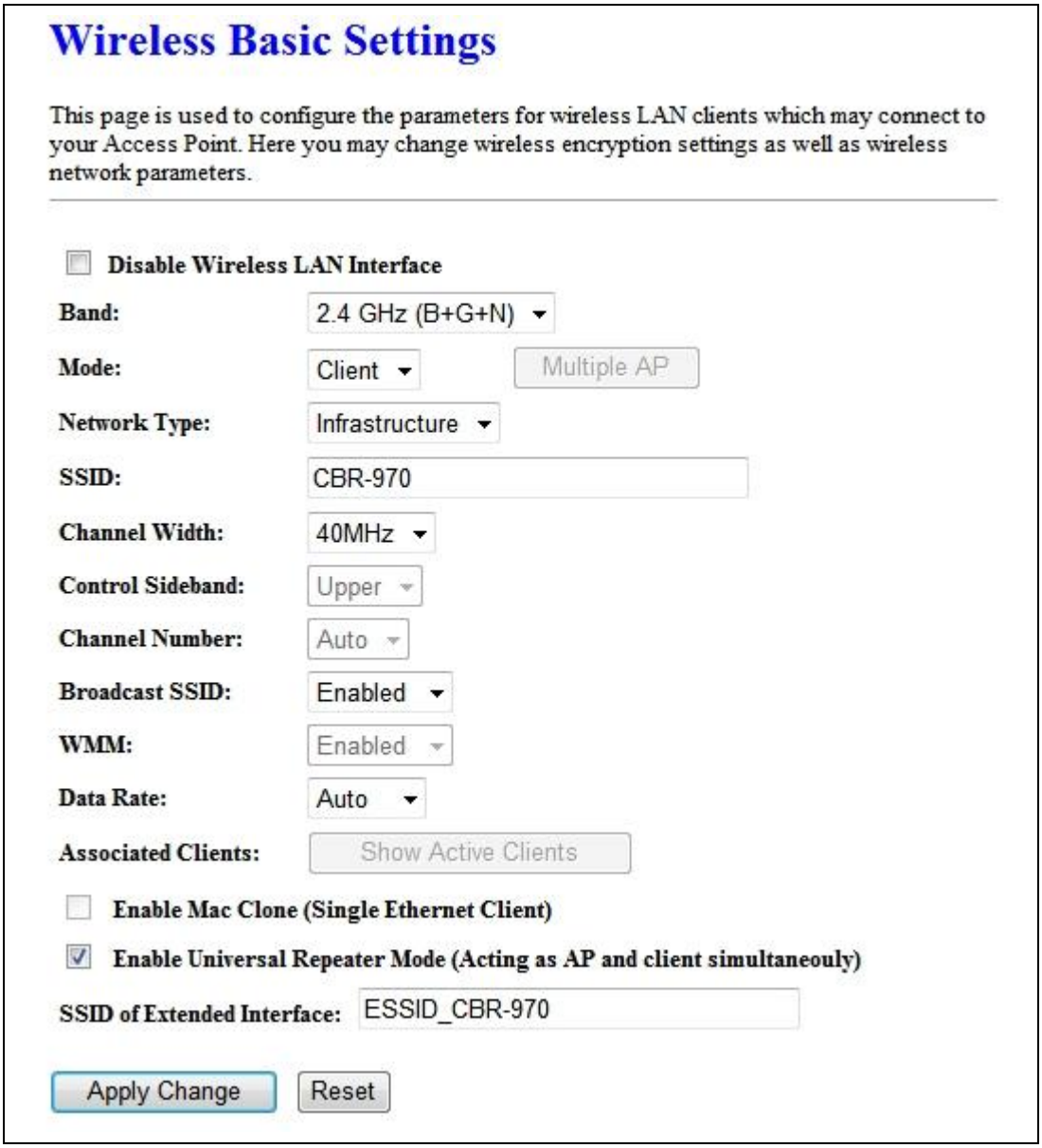
Item	Description
IP Address	The default IP address is **192.168.1.254**
Subnet Mask	Please enter the Subnet Mask address
Default Gateway	Please enter the Default Gateway address for LAN interface.
DHCP	Click to select **Disabled, Client** or **Server** in different operation mode of LAN access point.
DHCP Client Range	Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range
Static DHCP	Configures how static DHCP address are assigned to client (only available when DHCP server is enabled)
Device Name	Configures the device name of the router.
802.1d Spanning Tree	IEEE 802.1d **Spanning Tree Protocol** (**STP**) is a link layer network protocol that ensures a loop-free topology for any bridged LAN, This function is optional.
Clone MAC Address	If your ISP asks you to enter a specific MAC Address, please input the correct info at the column.
Apply Change & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

6.2 Wireless Setup

The category includes **Basic Settings**, **Advanced Settings**, **Site Survey**, **Security**, **Access Control**, and **WPS**. Please read below for the setting instructions.

6.2.1 Wireless Basic Setting

The basic settings related to the wireless are specified as following.



Item	Description
Disable Wireless LAN Interface	Turn off the wireless function.
Band	Please select the frequency. It has 6 options: 2.4 GHz (B/G/N/B+G/G+N/B+G+N).
Mode	In Wi-Fi AP mode only support Clint mode
Network Type	Please select the network type, it has 2 options: **Infrastructure** or **Ad hoc**.
SSID	Service Set identifier, the default SSID is **CBR-970/971**, users can define to any.
Channel Width	Please select the channel width, it has 2 options: 20MHZ, and 40MHZ.
Control Sideband	Enable this function will control your router use lower or upper channel.

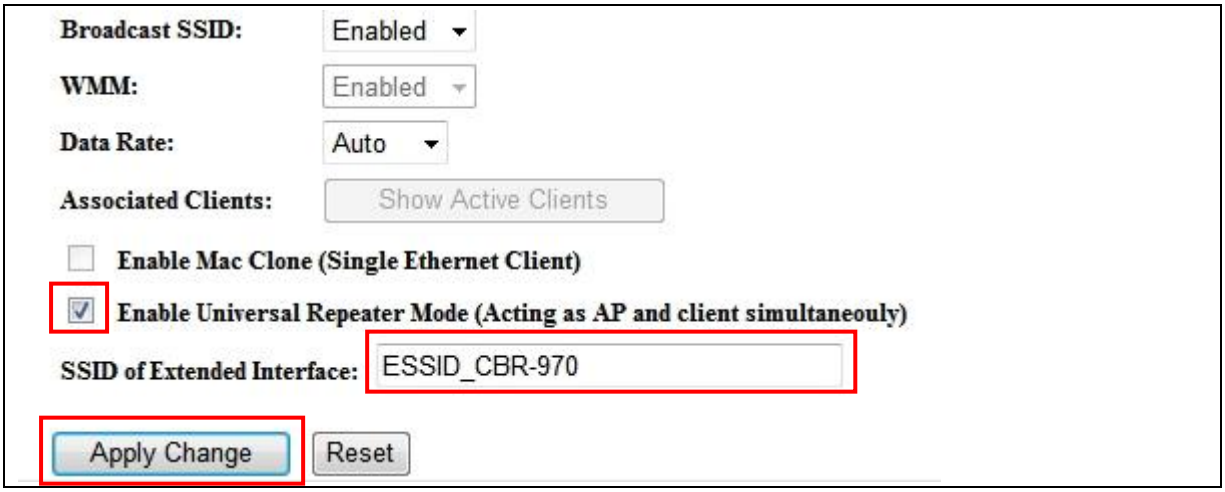
Broadcast SSID	User may choose to enable **Broadcast SSID** or not.
Data Rate	Please select the data transmission rate.
Associated Clients	Check the AP connectors and the Wireless connecting status.
Enable MAC Clone (Single Ethernet Client)	Clone the MAC address for ISP to identify.
Enable Universal Repeater Mode (Action as AP and Client **simultaneously**)	Allow to equip with the wireless way conjunction upper level, provide the bottom layer user link in wireless and wired way in the meantime. (Please check Note 1).
SSID of Extended Interface	While linking the upper level device in wireless way, you can set SSID to give the bottom layer user search.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

Note.

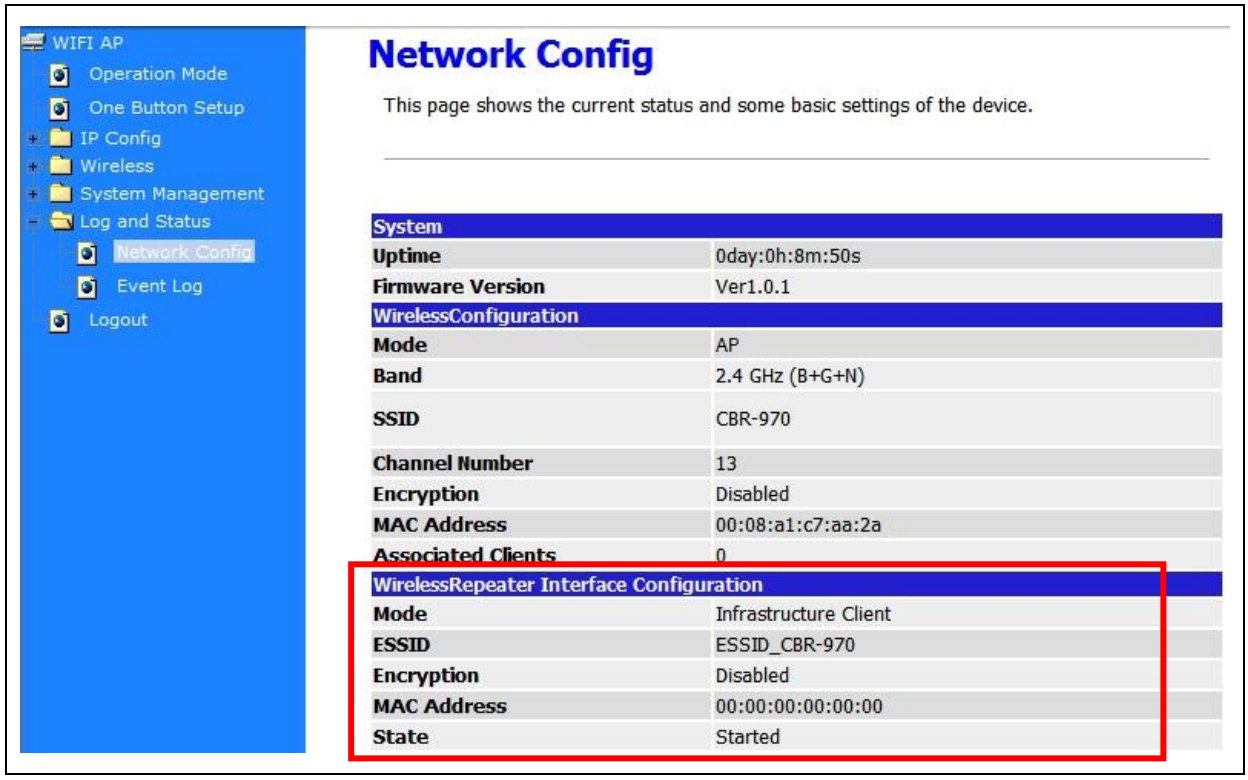
1. **Enable Universal Repeater Mode (Acting as AP and Client simultaneously)**

   Allow to equip with the wireless way conjunction upper level, provide the bottom layer user link in wireless and wired way in the meantime. (The IP that bottom layer obtains is from upper level.)

   Ex: When users enable the Universal Repeater to connect to the upper level device, please input the channel and SSID of the upper level device on router's GUI. Click on **Apply Changes** to save the settings. (The DHCP in IP config needs to be disabled.)



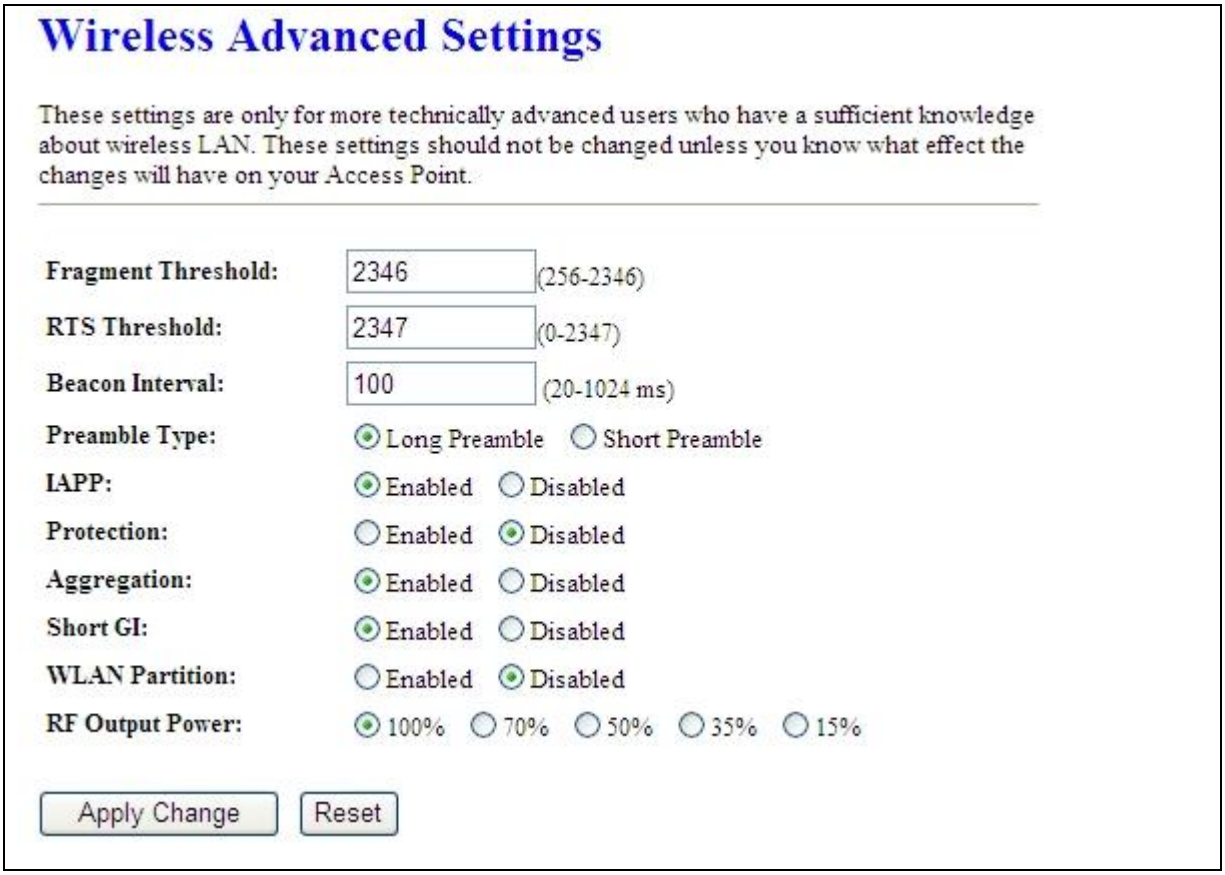
Users can go to the network Config section and check the information of upper level in Wireless Repeater Interface Configuration.



Caution: when users enable the wireless encryption. The upper level and lower devices can connect to each other even if their encryption types are not the same.

6.2.2 Wireless Advanced Settings

Please complete the wireless advanced settings as following instructions.


Wireless Advanced Settings
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.
Fragment Threshold: 2346 (256-2346)
RTS Threshold: 2347 (0-2347)
Beacon Interval: 100 (20-1024 ms)
Preamble Type: Long Preamble Short Preamble
IAPP: Enabled Disabled
Protection: Enabled Disabled
Aggregation: Enabled Disabled
Short GI: Enabled Disabled
WLAN Partition: Enabled Disabled
RF Output Power: 100% 70% 50% 35% 15%
Apply Change
Reset

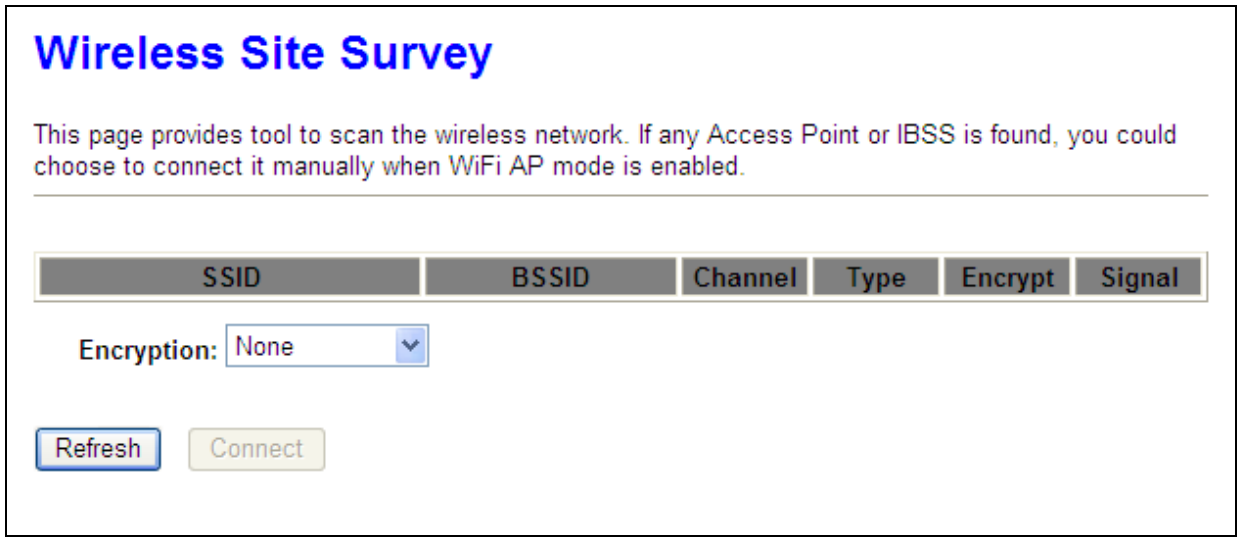
Item	Description
Fragment Threshold	To identify the maxima length of packet, the over length packet will be fragmentized. The allowed range is 256-2346, and default length is 2346 Bytes.
RTS Threshold	This value should remain at its default setting of 2347. The range is 0~2347. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the present RTS threshold size, the RTS/CTS mechanism will not be enabled. The router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. Fill the range from 0 to 2347 into this blank.
Beacon Interval	Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. The allowed setting range is 20-1024 ms.
Preamble Type	Preamble is the first subfield of PPDU, which is the appropriate frame format form transmission to PHY (Physical layer). There are two options, Short Preamble and Long Preamble. The Short Preamble

	option improves throughput performance. Select the suit Preamble as Short or Long Preamble.
IAPP	Inter Access Point Protocol. Allow seamless roaming between Access Points in your wireless network.
Protection	Please select to enable wireless protection or not.
Aggregation	Enable this function will combine several packets to one and transmit it. It can reduce the problem when mass packets are transmitting.
Short GI	Users can get better wireless transmission efficiency when they enable this function.
RF Output Power	Users can adjust the RF output power to get the best wireless connection. Users can choose from 100%, 70%, 50%, 35%, and 15%.
Apply Changes & Reset	Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

6.2.3 Wireless Site Survey

This function provides users to search existing wireless APs or wireless base stations from ISP. You can connect to a wireless AP manually in Wi-Fi AP mode. The designed AP will appear on SSID column in Wireless Basic Setup page.

Please click on **Refresh** to refresh the list. Click **Connect** after select an existing AP to connect.



6.2.4 Wireless Security Setup

4 encryption types could be selected here, please follow below instructions for the setting. (This is for setting up the AP, not for the client)

Wireless Security Setup
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.
Select SSID:
Root AP - CBR-970
Apply Change
Reset
Encryption:
Disable
802.1x Authentication:

1. Encryption – WEP

1.1 Set WEP Key

This section provides 64bit and 128bit WEP encryptions for wireless network. Users can also choose ASCII and Hex shared Key format to protect data.

1.2 802.1x Authentication

It is a safety system by using authentication to protect your wireless network.

Please choose between WEP 64bits and WEP 128bits.

2. Encryption – WPA（WPA、WPA2 & WPA2 Mixed）

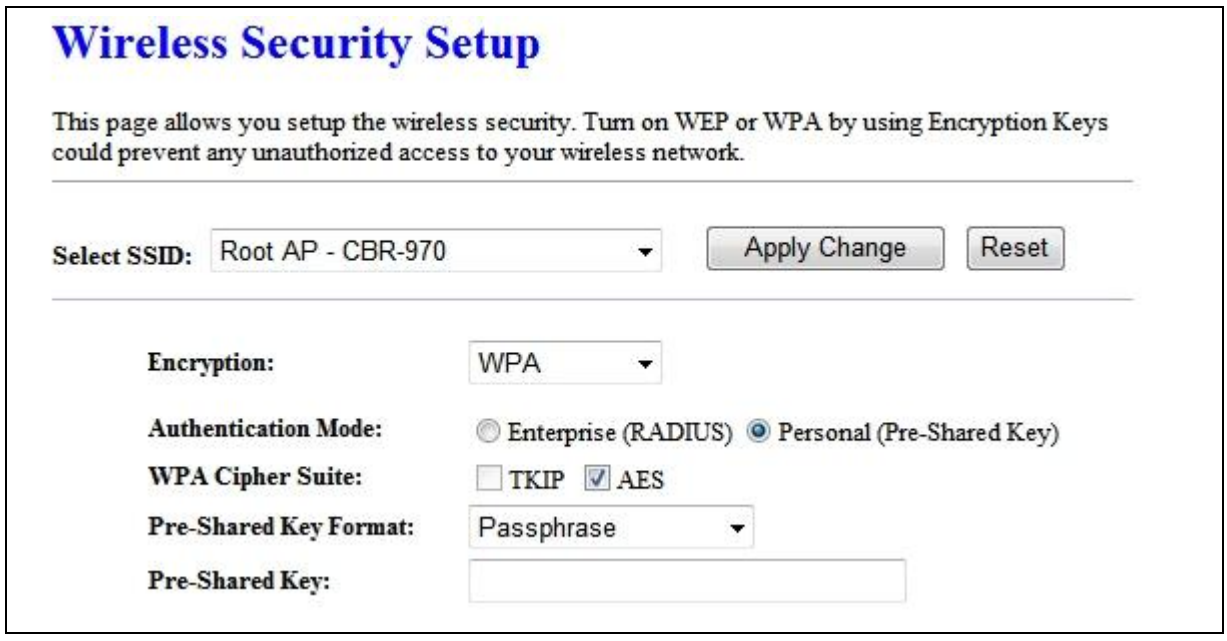
WPA Authentication Mode

2.1 Enterprise (RADIUS)

Please input the Port, IP Address, and Password of Authentication RADIUS Server.

2.2 Personal（Pre-Shared Key）

Pre-Shared Key type is ASCII Code; the length is between 8 to 63 characters. If the key type is Hex, the key length is 64 characters.



3. Apply Changes & Reset

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

6.2.5 Wireless Access Control

The function of access control is to allow or deny users to access the router by according MAC address, it is optional. If you select **Allowed Listed**, then only those clients whose MAC address is listed on access control can connect to your base station. If you select **Deny Listed**, those clients whose MAC address is listed on access control can't connect to your base station.

Wireless Access Control
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.
Wireless Access Control Mode:
Disable
Users may enable or disable this function.
MAC Address:
Comment:
Apply Change
Reset
Current Access Control List:
MAC Address
Comment
Select
Delete Selected
Delete All
Reset

Take the wireless card as the example.

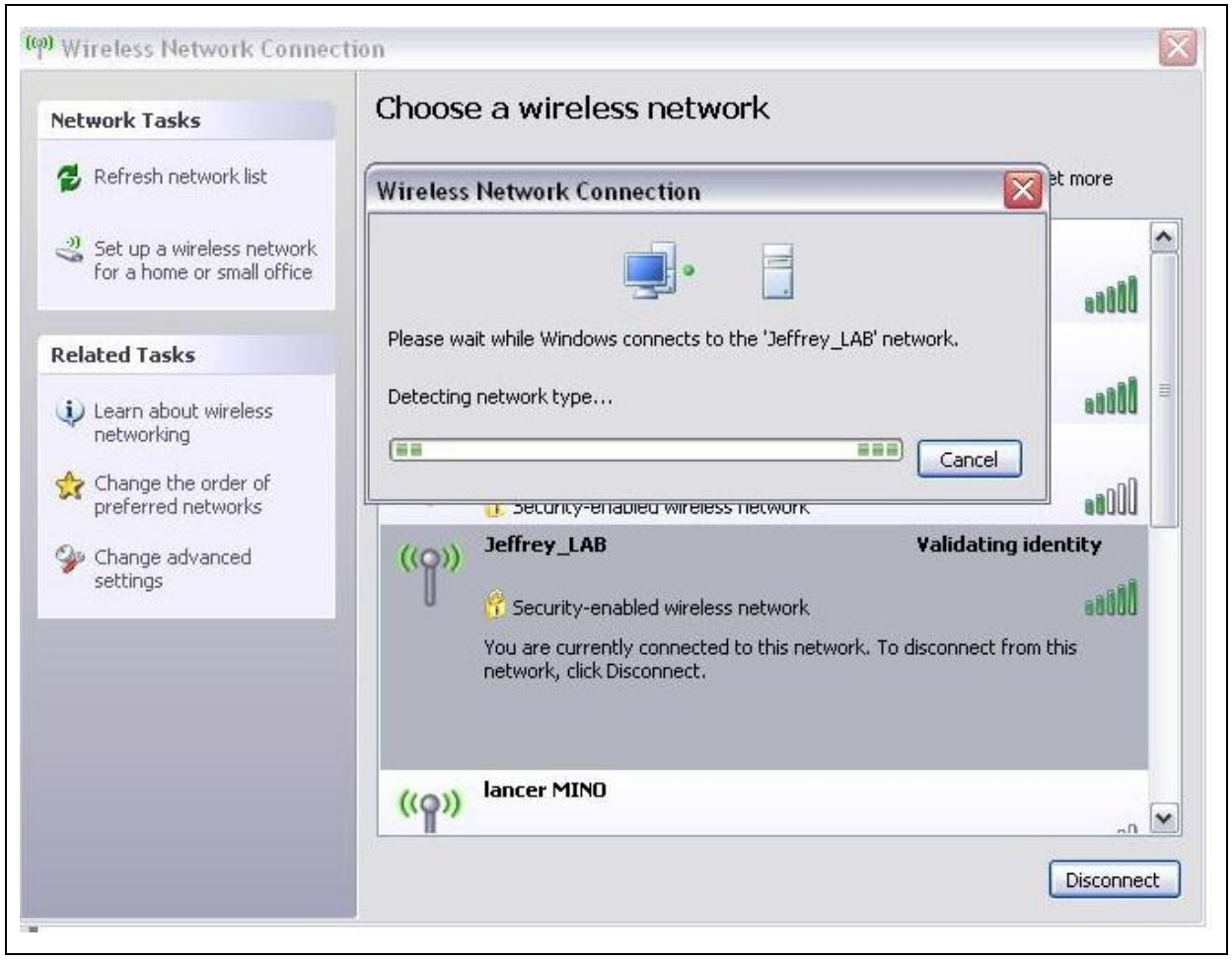
(1) We will use **Deny Listed** as an example. Please select **Deny Listed** in **Wireless Access Control Mode** first, and then input the MAC address of wireless card in MAC Address field. Click **Apply Changes** to save the setting data.

Wireless Access Control
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.
Wireless Access Control Mode:
Deny Listed
MAC Address:
00D041B0D117
Comment:
Apply Changes
Reset
Current Access Control List:
MAC Address
Comment
Select
Delete Selected
Delete All
Reset

(2) You will find out that the MAC address appears on **Current Access Control List**, it means the initiation is completed.

Wireless Access Control
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.
Wireless Access Control Mode:
Deny Listed
MAC Address:
Comment:
Apply Changes
Reset
Current Access Control List:
MAC Address
Comment
Select
00:d0:41:b0:d1:17
Delete Selected
Delete All
Reset

(3) Please open wireless card UI and try to connect to this router. You will find out that the connection request will be denied.


Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Wireless Network Connection
Please wait while Windows connects to the 'Jeffrey_LAB' network.
Detecting network type...
Cancel
Jeffrey_LAB
Validating identity
Security-enabled wireless network
You are currently connected to this network. To disconnect from this network, click Disconnect.
lancer MINO
Disconnect

6.2.6 WPS Setting

Please refer to Chapter **4.2.6** for detailed WPS configuration methods.

6.3 System Management

It has 6 sections: Change Password, Firmware Upgrade, Profiles Save, Time Zone Setting, UPnP Setting, and Language Setting. It is easy and helpful for users making more detailed settings.

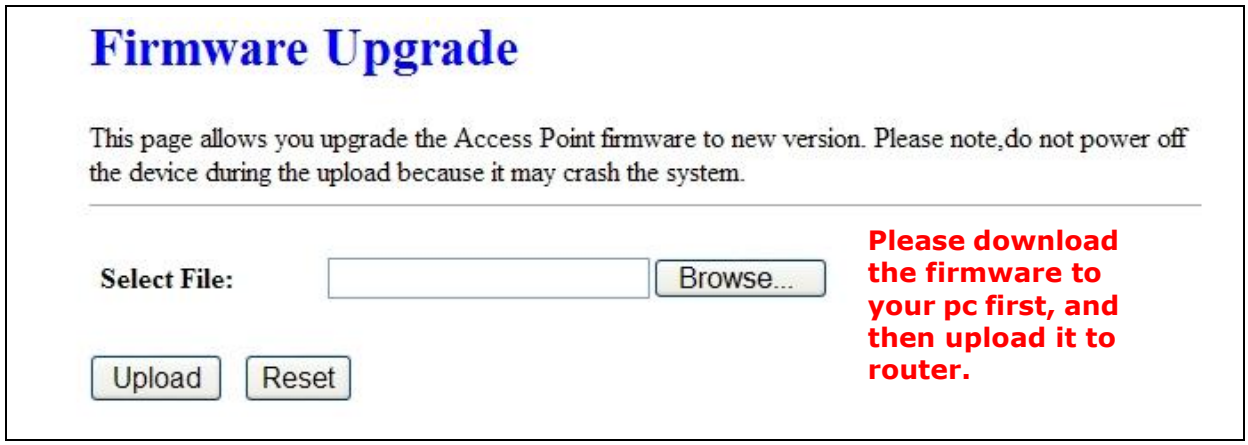
6.3.1 Change Password

Users can set or change their password in this section.

Click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data.

6.3.2 Firmware Upgrade

This function can upgrade the firmware of the router. There is certain risk while doing firmware upgrading. Firmware upgrade is not recommended unless the significant faulty is found and published on official website. If you feel the router has unusual behaviors and is not caused by the ISP and environment. You can check the website (http://www.cnet.com.tw) to see if there is any later version of firmware. Download the firmware to your computer, click **Browser** and point to the new firmware file. Click **Upload** to upgrade the firmware. You can't make any move unless the machine reboot completely.

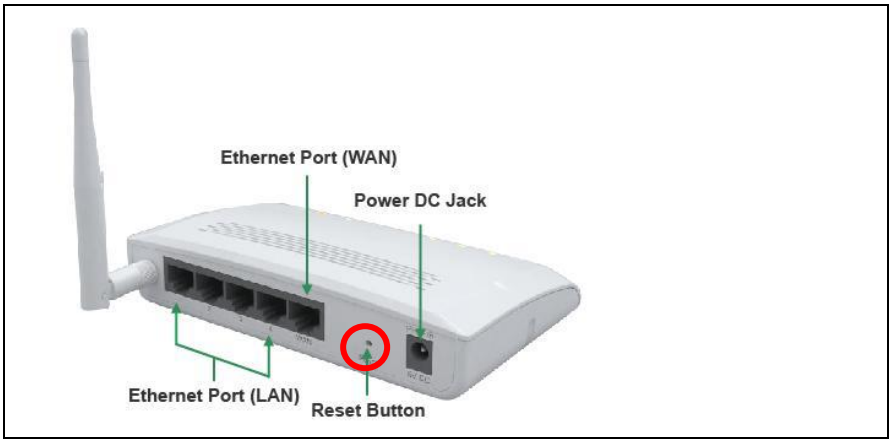

Firmware Upgrade
This page allows you upgrade the Access Point firmware to new version. Please note,do not power off the device during the upload because it may crash the system.
Select File:
Browse...
Upload
Reset
Please download the firmware to your pc first, and then upload it to router.

Caution: To prevent that firmware upgrading is interrupted by other wireless signals and causes failure. We recommend users to use wired connection during upgrading.

Caution: The firmware upgrade will not remove your previous settings.

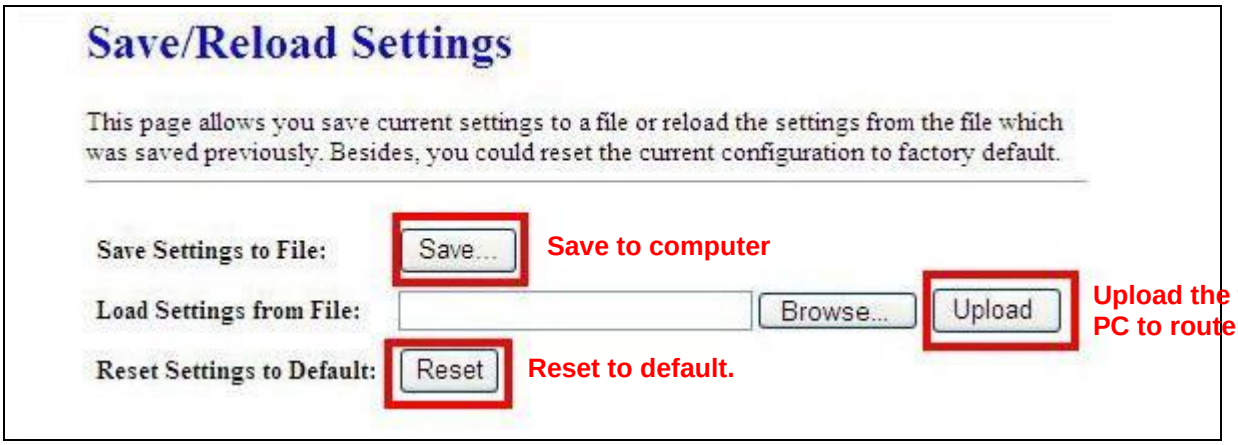
* Reset button:

On the front of this router, there is a reset button. If you cannot login the administrator page by forgetting your password; or the router has problem you can't solve. You can push the reset button for 5 seconds with a stick. The router will reboot and all settings will be restored to factory default settings. If the problem still exists, you can visit our web site to see if there is any firmware for download to solve the problem.



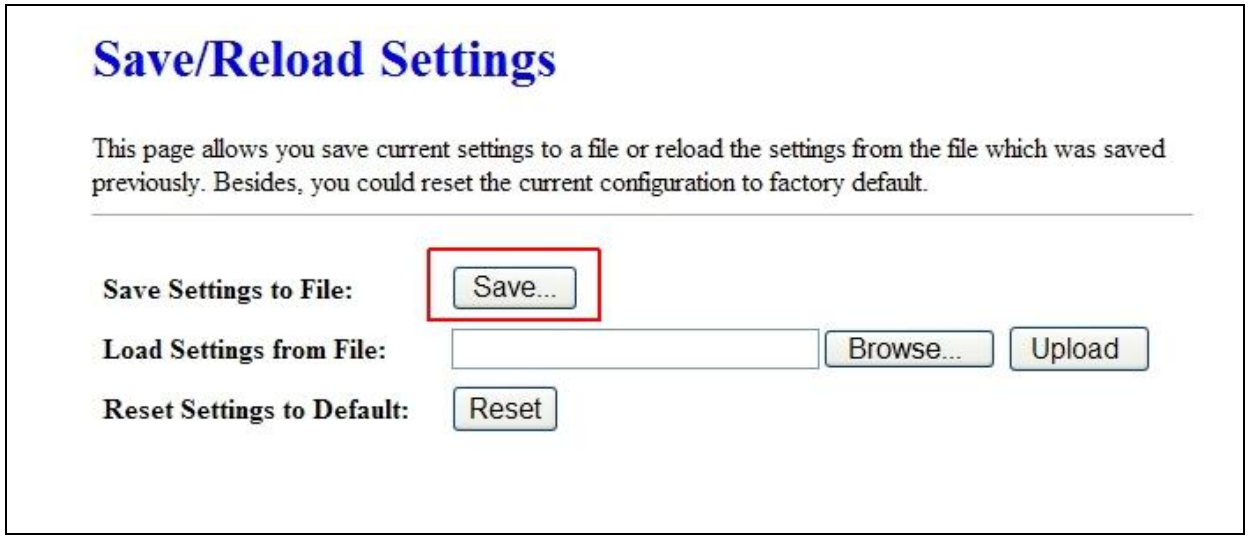
6.3.1 Profile Save

Users can create a backup file that contains current router settings. This backup file can be used to restore router settings. This is especially useful in the event you need to reset the router to its default settings.

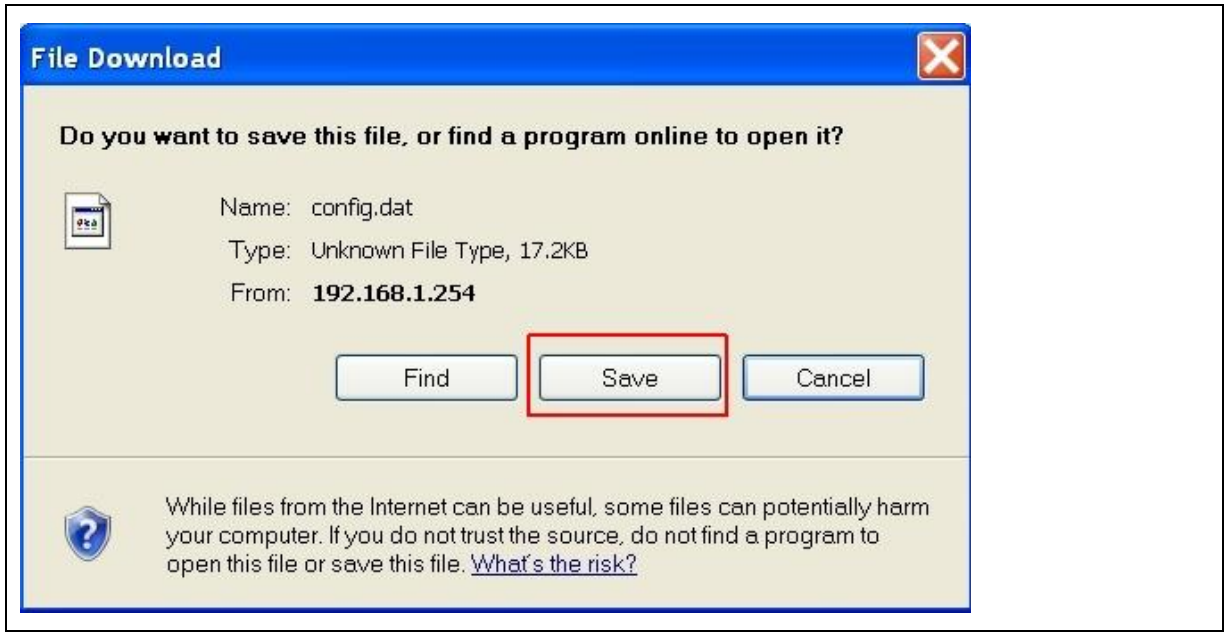

Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Save to computer
Load Settings from File:
Browse...
Upload
Upload the file from PC to router
Reset Settings to Default:
Reset
Reset to default.

a. Save Configuration

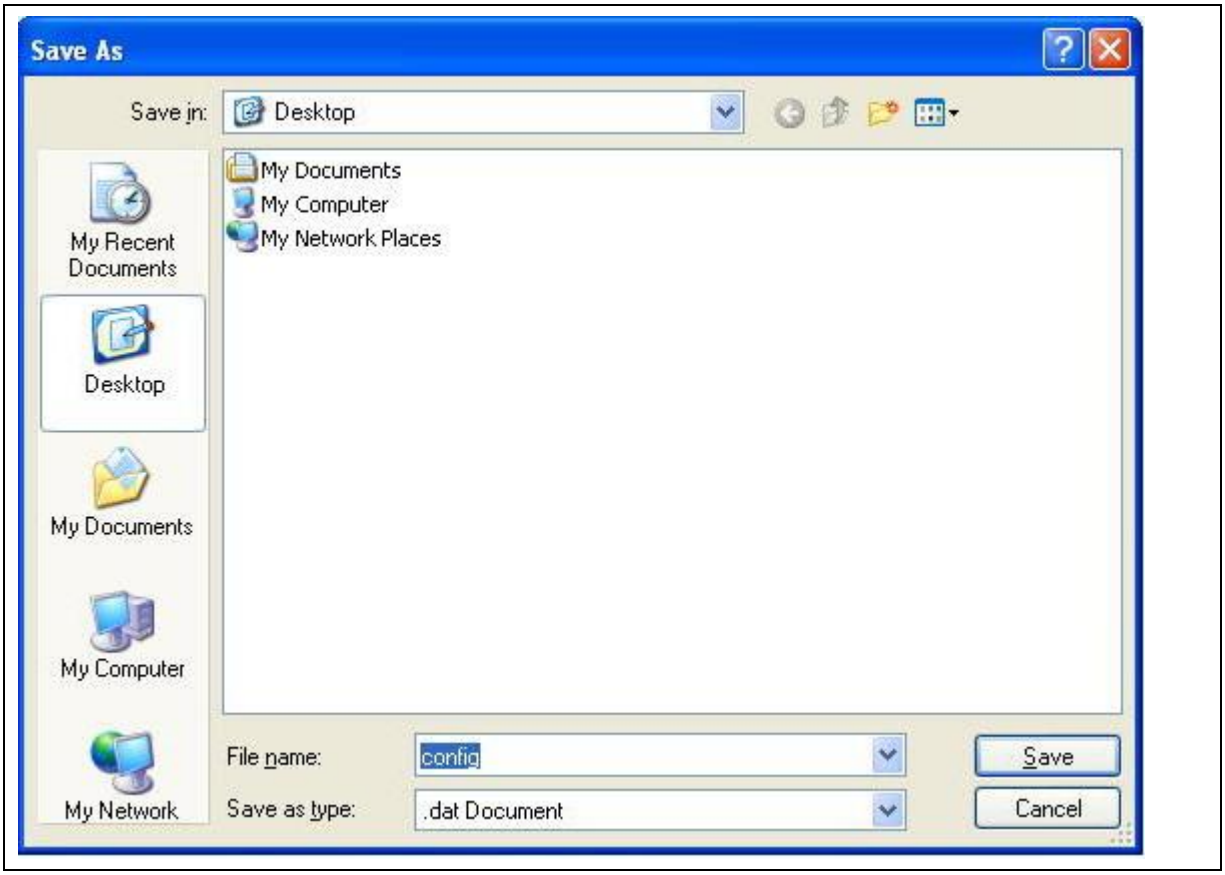
(1) Click **Save**


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Browse...
Upload
Reset Settings to Default:
Reset

(2) Please click “Save” to save the configuration to your computer.

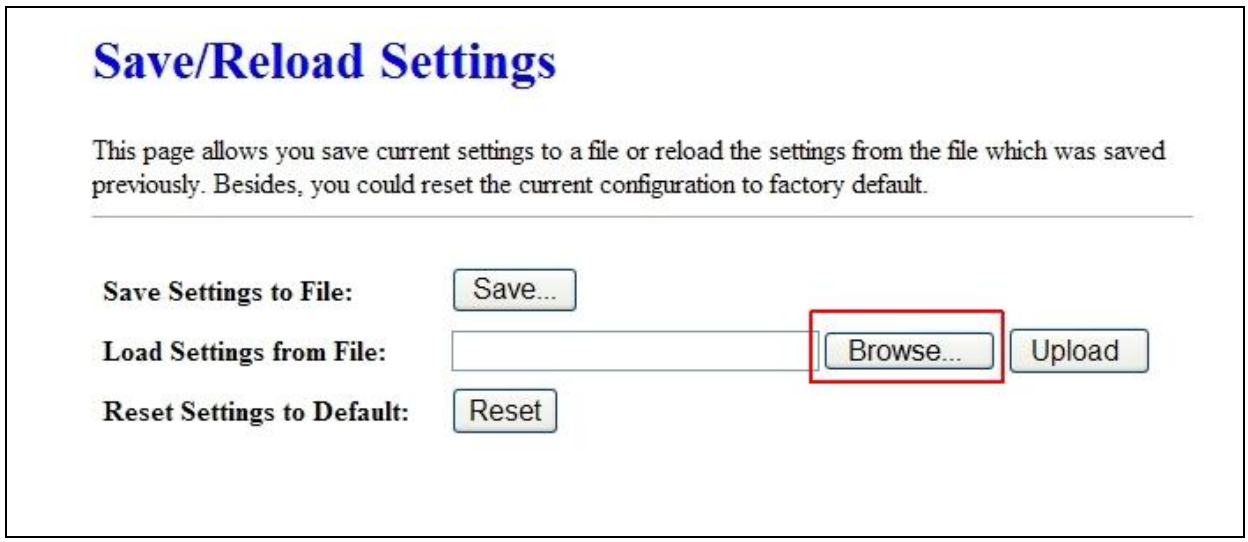

File Download
Do you want to save this file, or find a program online to open it?
Name: config.dat
Type: Unknown File Type, 17.2KB
From: 192.168.1.254
Find
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

(3) Select the location which you want to save file, then click **Save.**

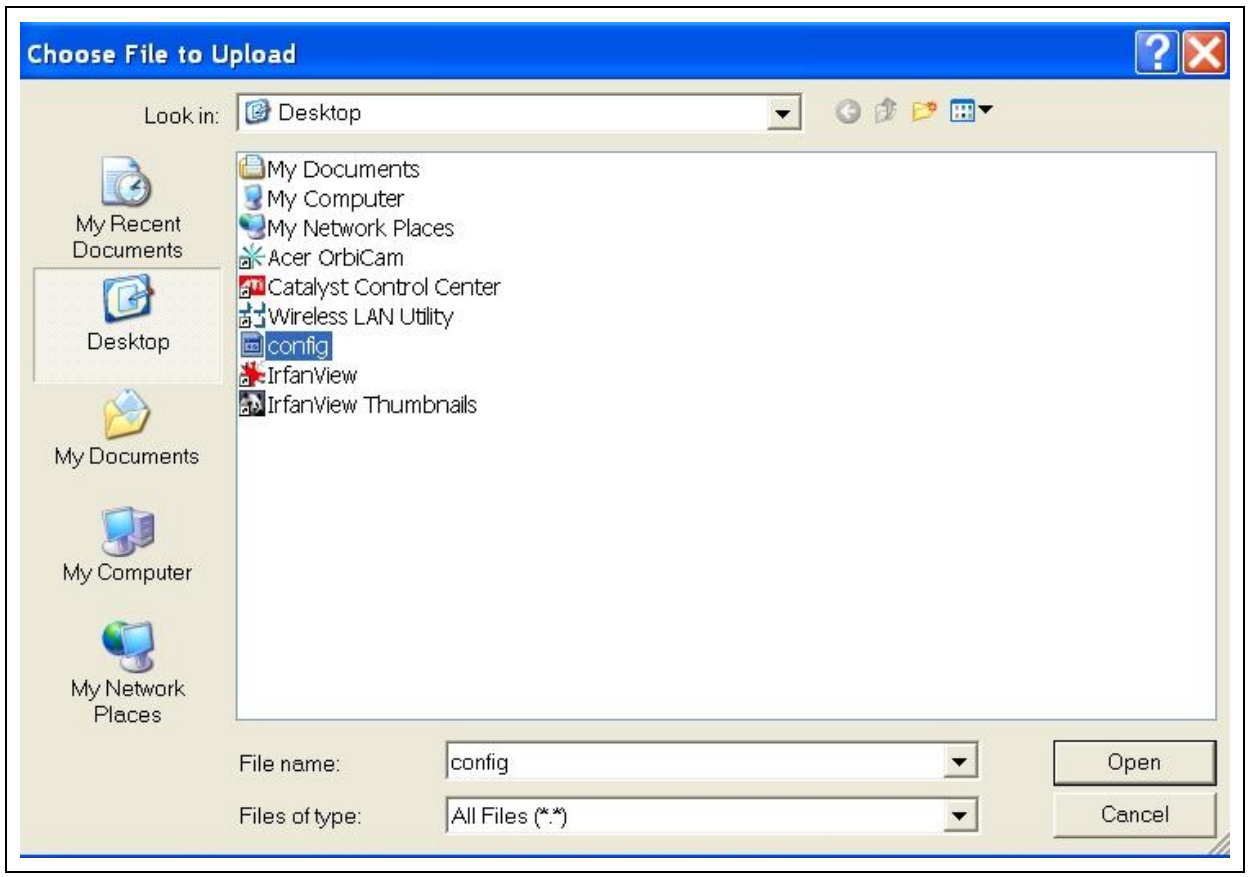


b. Load configuration file

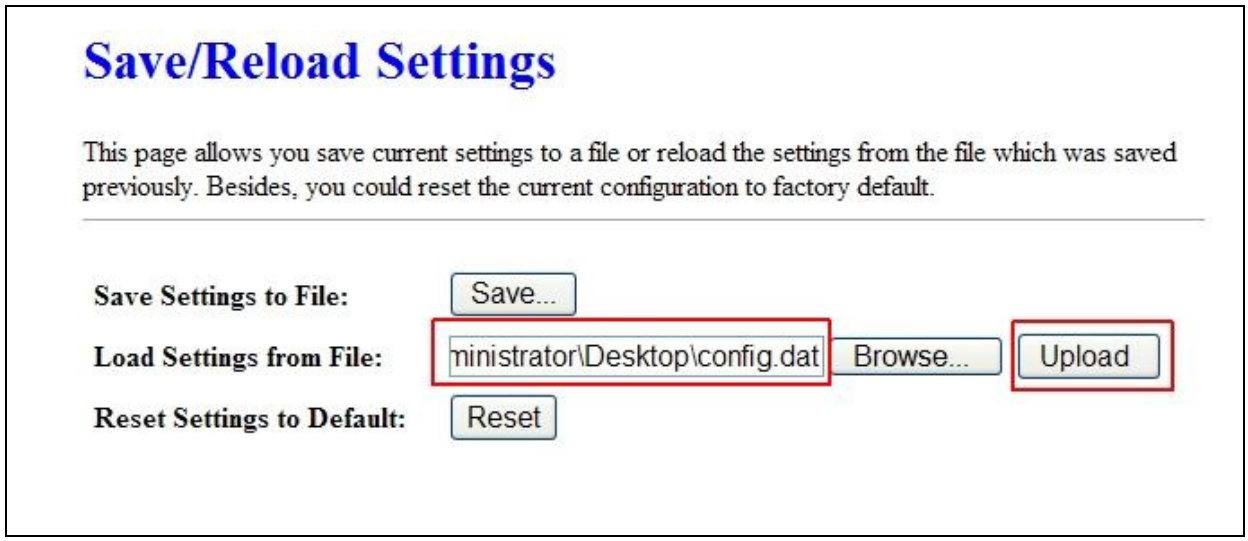
(1) Click **Browser**


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Browse...
Upload
Reset Settings to Default:
Reset

(2) Select configuration file then click **Open**



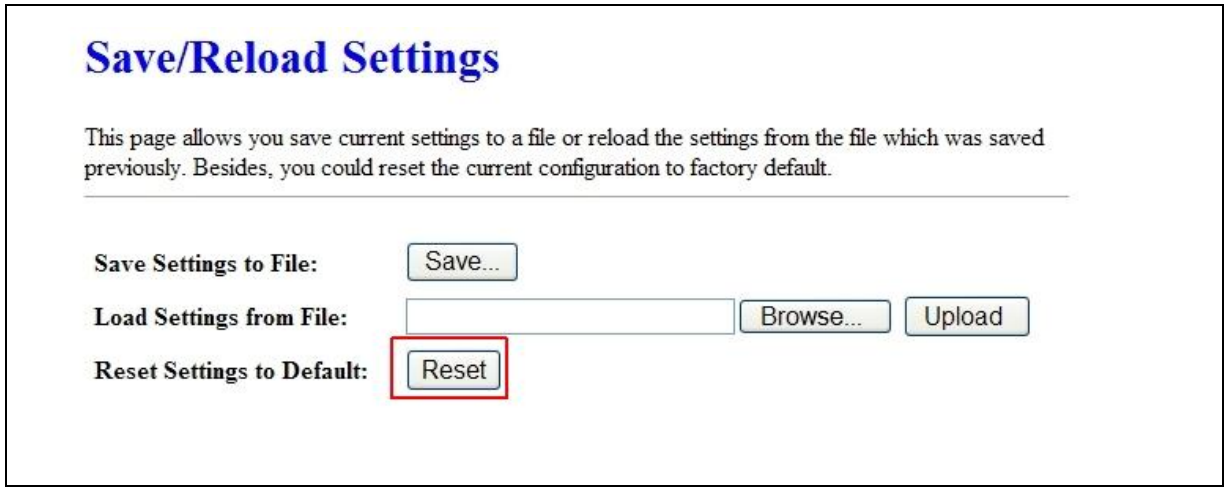
(3) Click **Upload** to upload configuration file to CBR-970/971.


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
ministrator\Desktop\config.dat
Browse...
Upload
Reset Settings to Default:
Reset

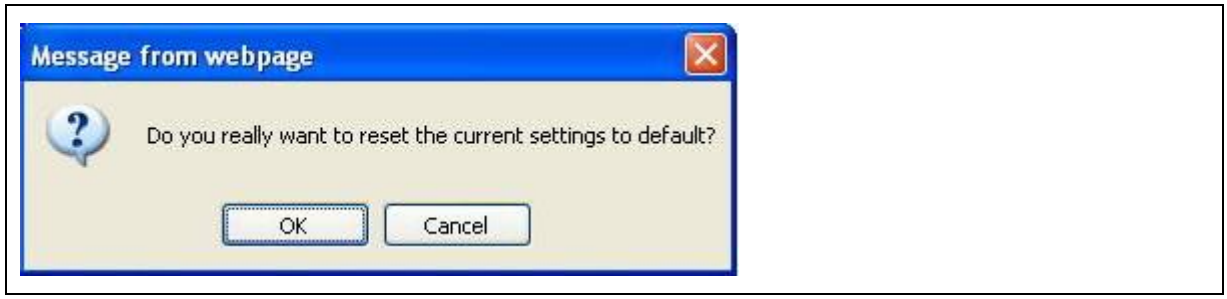
(4) After 90 seconds, CBR-970/971 will reboot automatically.

(C) Reload factory default setting

1. Please click **Reset**


Save/Reload Settings
This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.
Save Settings to File:
Save...
Load Settings from File:
Browse...
Upload
Reset Settings to Default:
Reset

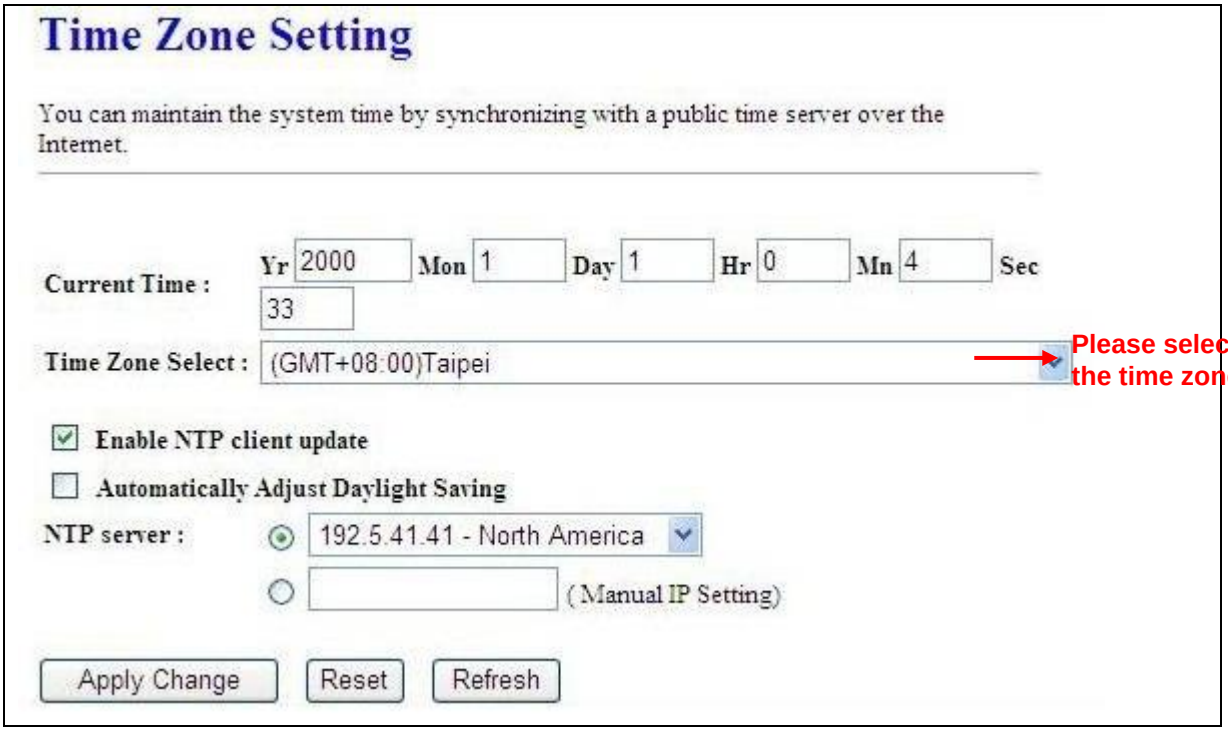
(2) Please click **OK** to start reload factory default setting to CBR-970/971.



(3) After 90 seconds, CBR-970/971 will reboot automatically.

6.3.2 Time Zone Setting

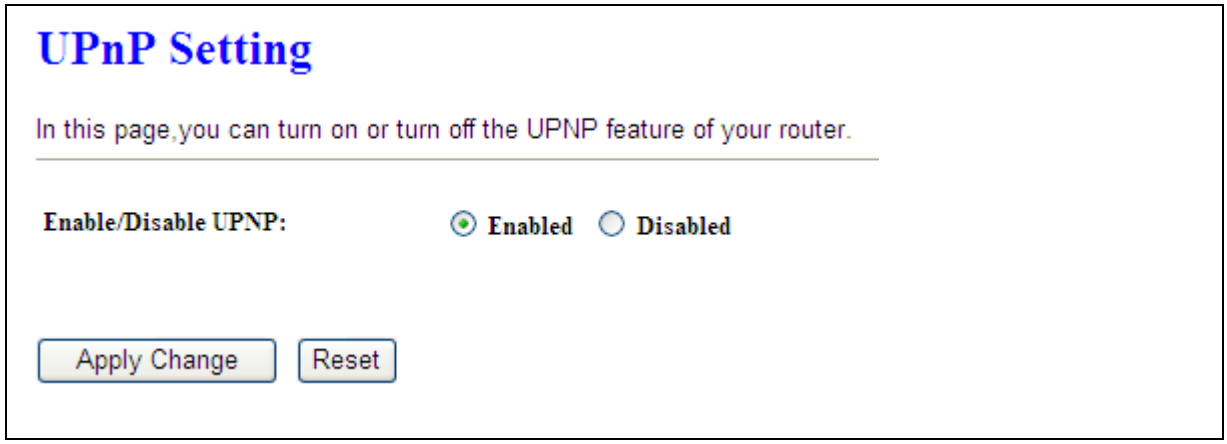
Users can synchronize the local clock on the router to an available NTP server (optional). To complete this setting, enable NTP client update and select the correct Time Zone.


Time Zone Setting
You can maintain the system time by synchronizing with a public time server over the Internet.
Current Time :
Yr 2000 Mon 1 Day 1 Hr 0 Mn 4 Sec 33
Time Zone Select :
(GMT+08:00)Taipei
Please select the time zone
Enable NTP client update
Automatically Adjust Daylight Saving
NTP server :
192.5.41.41 - North America
(Manual IP Setting)
Apply Change
Reset
Refresh

Item	Description
Current Time	Users can input the time manually.
Time Zone Select	Please select the time zone.
Enable NTP client update	Please select to enable NTP client update or not.
Automatically Adjust Daylight Saving	Please select to enable **Automatically Adjust Daylight Saving** or not.
NTP Server	Please select the NTP server from the pull-down list, or you can enter the NTP server IP address manually.
Apply Changes & Reset & Refresh	Please click on **Apply Changes** to save the setting data. Or you may click on **Reset** to clear all the input data. Or you may click on **Refresh** to update the system time on the screen.

6.3.3 UPnP Setting

Universal Plug and Play (**UPnP**) is a standard of networking protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. CBR-970/971 supports UPnP function, and can cooperate with other UPnP devices. When you activate UPnP, please click **My Network Places**. Users will see an **Internet Gateway Device** icon. By click the icon, users can enter the GUI of the router. If you do not wish to use UPnP, you can disable it.

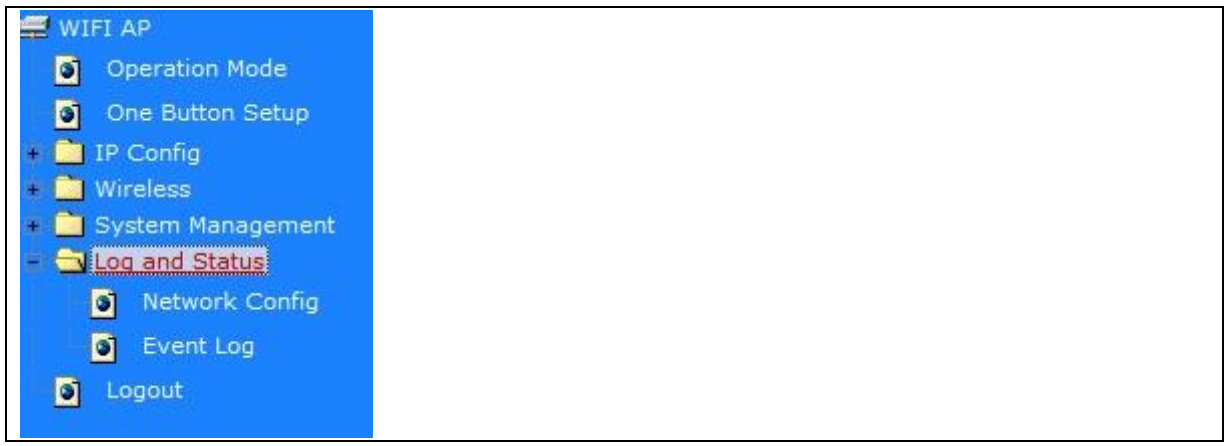


*Enable/Disable UPnP

Select to enable or disable this function.

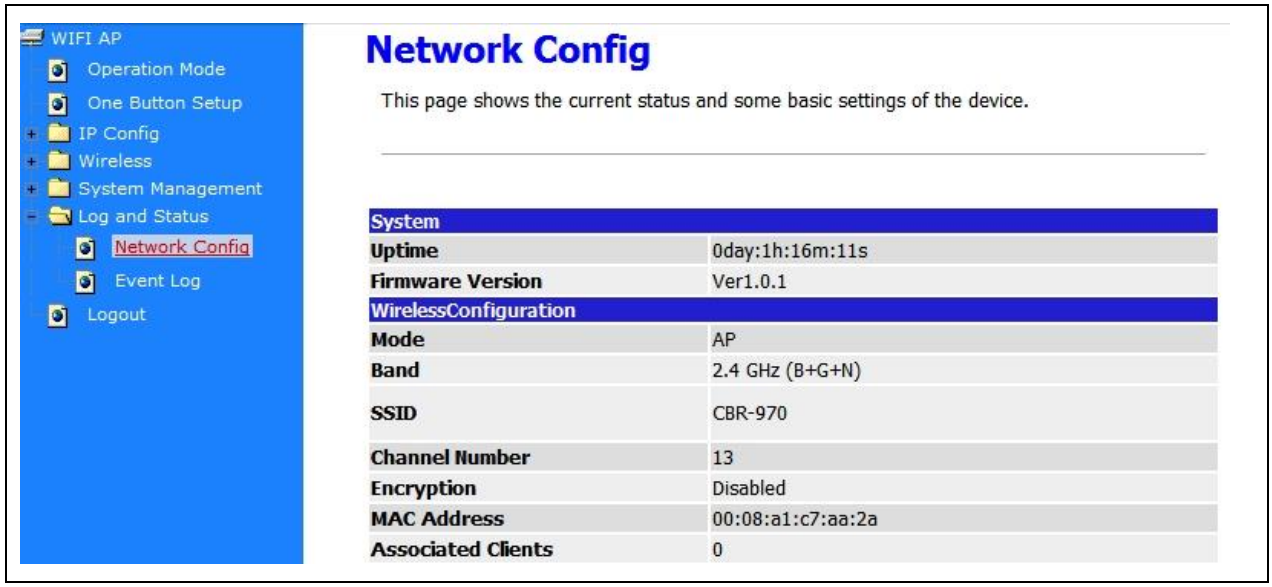
6.4 Log & Status

The category provides **Network Config** and **Event Log** status for users to know the operation status.



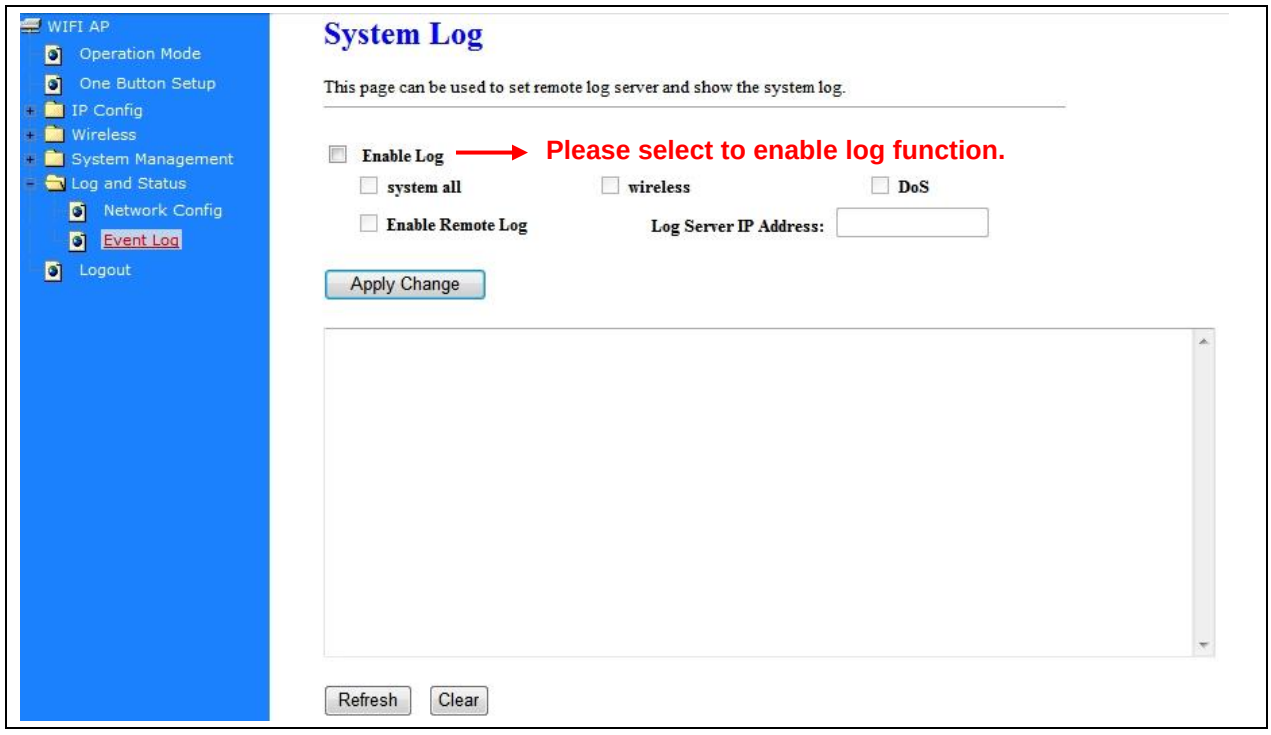
6.4.1 Network Config

Users can check the Internet status under this category, including Firmware version, Wireless setting, Connecting Time, WAN, TCP/IP …information.



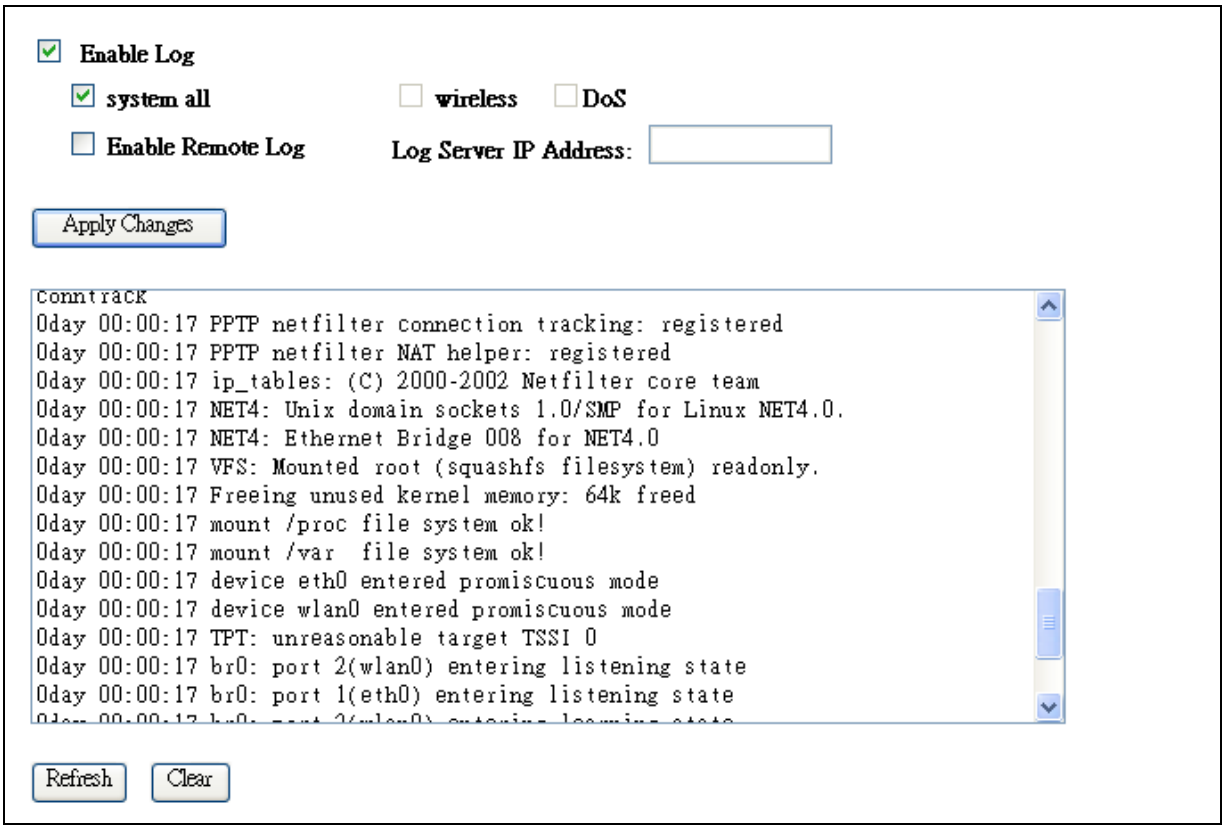
6.4.2 Event Log

You may enable the event log feature here.



Item	Description
Enable Log	You may choose to enable Event Log or not.
System all, Wireless, & DoS	Please select the event you want to record.
Enable Remote Log	You may choose to enable the remote event log or not.
Log Server IP Address	Please input the log server IP Address.
Apply Changes & Refresh & Clear	Click on **Apply Changes** to save the setting data. Click on **Refresh** to renew the system time, or on **Clear** to clear all the record.

* The following figure is an example when users click **Apply Changes** to record the event log.


Enable Log
system all
wireless
DoS
Enable Remote Log
Log Server IP Address:
Apply Changes
Conntrack
0day 00:00:17 PPTP netfilter connection tracking: registered
0day 00:00:17 PPTP netfilter NAT helper: registered
0day 00:00:17 ip_tables: (C) 2000-2002 Netfilter core team
0day 00:00:17 NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
0day 00:00:17 NET4: Ethernet Bridge 008 for NET4.0
0day 00:00:17 VFS: Mounted root (squashfs filesystem) readonly.
0day 00:00:17 Freeing unused kernel memory: 64k freed
0day 00:00:17 mount /proc file system ok!
0day 00:00:17 mount /var file system ok!
0day 00:00:17 device eth0 entered promiscuous mode
0day 00:00:17 device wlan0 entered promiscuous mode
0day 00:00:17 TPT: unreasonable target TSSI 0
0day 00:00:17 br0: port 2(wlan0) entering listening state
0day 00:00:17 br0: port 1(eth0) entering listening state
Refresh
Clear

6.5 Logout

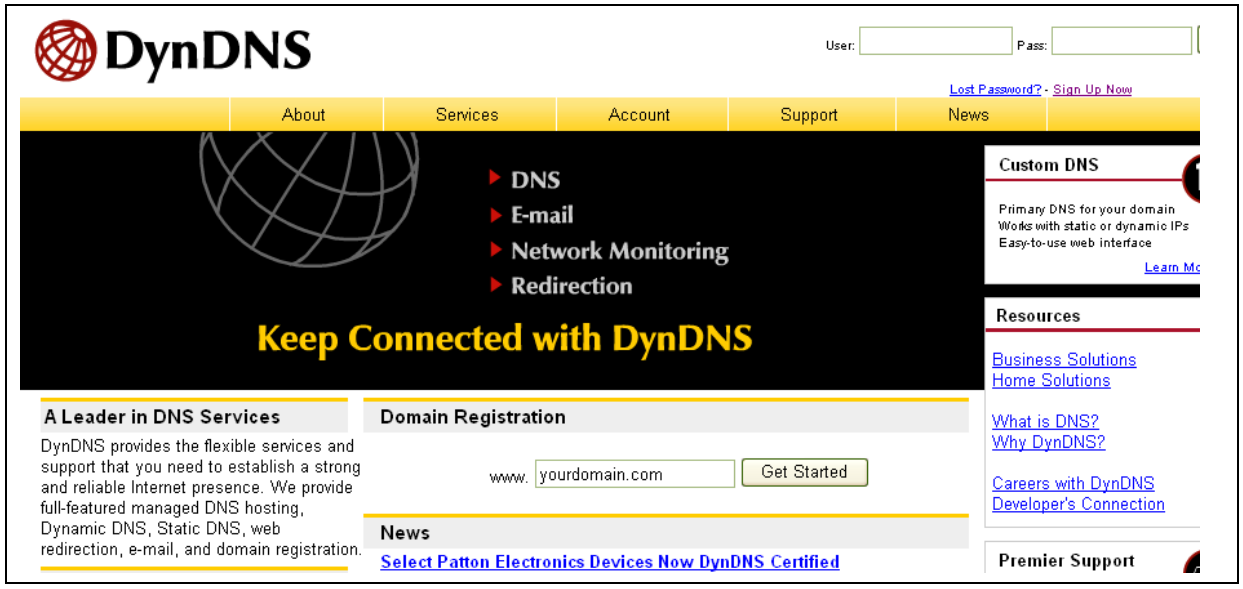
This function logs out the user.

Chapter 7 DDNS Account Setup

You can assign a fixed host and domain name to a dynamic Internet IP address. Each time the router boots up, it will re-register its domain-name-to-IP-address mapping with the DDNS service provider. This is the way Internet users can access the router through a domain name instead of its IP address.

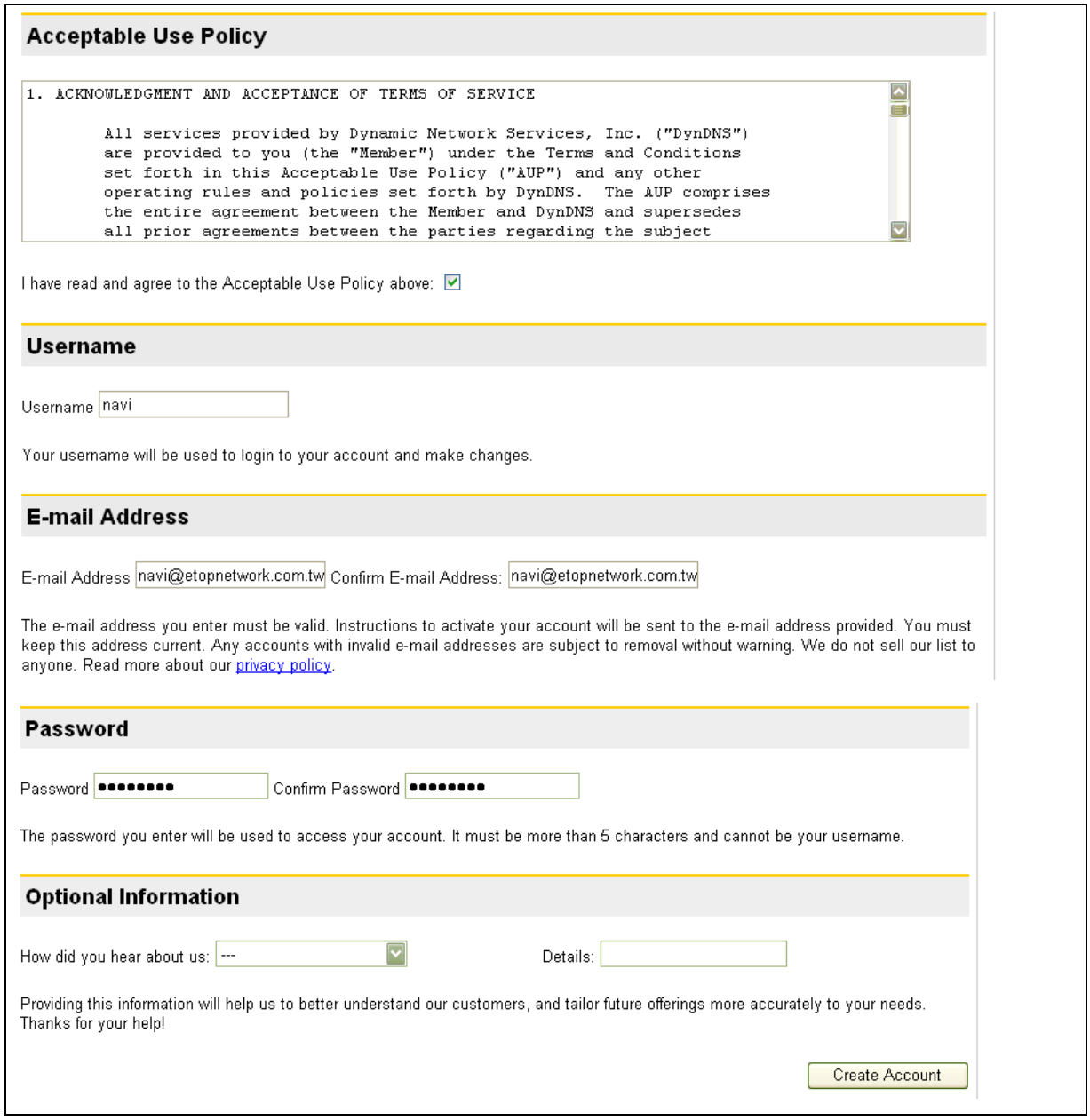
【Step 1】

Please visit the website http://www.dyndns.com/, and click on **Sign Up Now**.



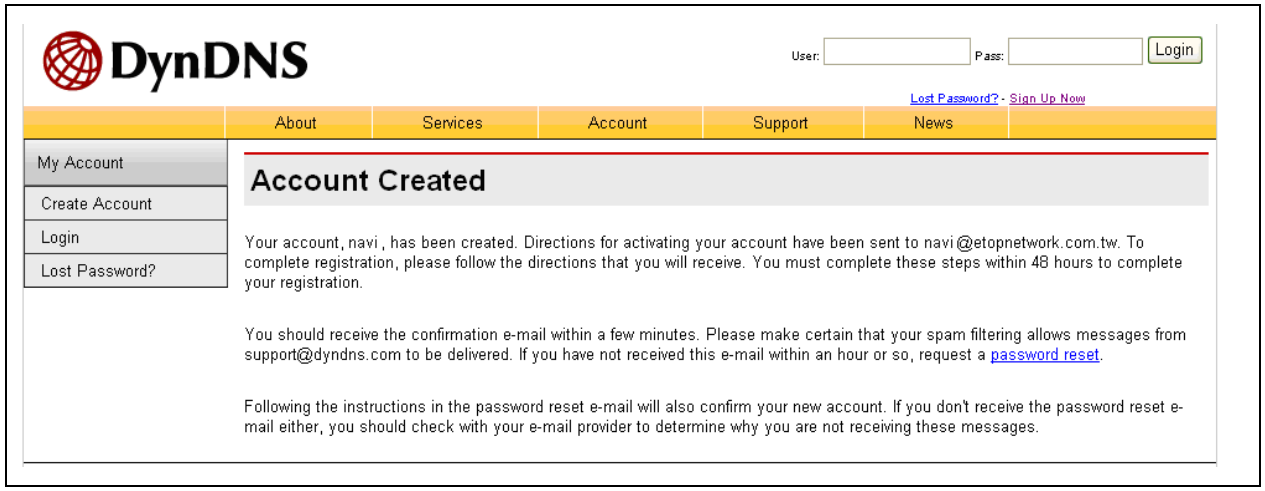
【Step 2】

Please fulfill the requested information at the column, and click on **Create Account** when finished. (The information shown on the screen is for your reference only)


Acceptable Use Policy
1. ACKNOWLEDGMENT AND ACCEPTANCE OF TERMS OF SERVICE
All services provided by Dynamic Network Services, Inc. ("DynDNS")
are provided to you (the "Member") under the Terms and Conditions
set forth in this Acceptable Use Policy ("AUP") and any other
operating rules and policies set forth by DynDNS. The AUP comprises
the entire agreement between the Member and DynDNS and supersedes
all prior agreements between the parties regarding the subject
I have read and agree to the Acceptable Use Policy above:
Username
Username navi
Your username will be used to login to your account and make changes.
E-mail Address
E-mail Address navi@etopnetwork.com.tw Confirm E-mail Address: navi@etopnetwork.com.tw
The e-mail address you enter must be valid. Instructions to activate your account will be sent to the e-mail address provided. You must keep this address current. Any accounts with invalid e-mail addresses are subject to removal without warning. We do not sell our list to anyone. Read more about our privacy policy.
Password
Password Confirm Password
The password you enter will be used to access your account. It must be more than 5 characters and cannot be your username.
Optional Information
How did you hear about us: ---
Details:
Providing this information will help us to better understand our customers, and tailor future offerings more accurately to your needs. Thanks for your help!
Create Account

【Step 3】

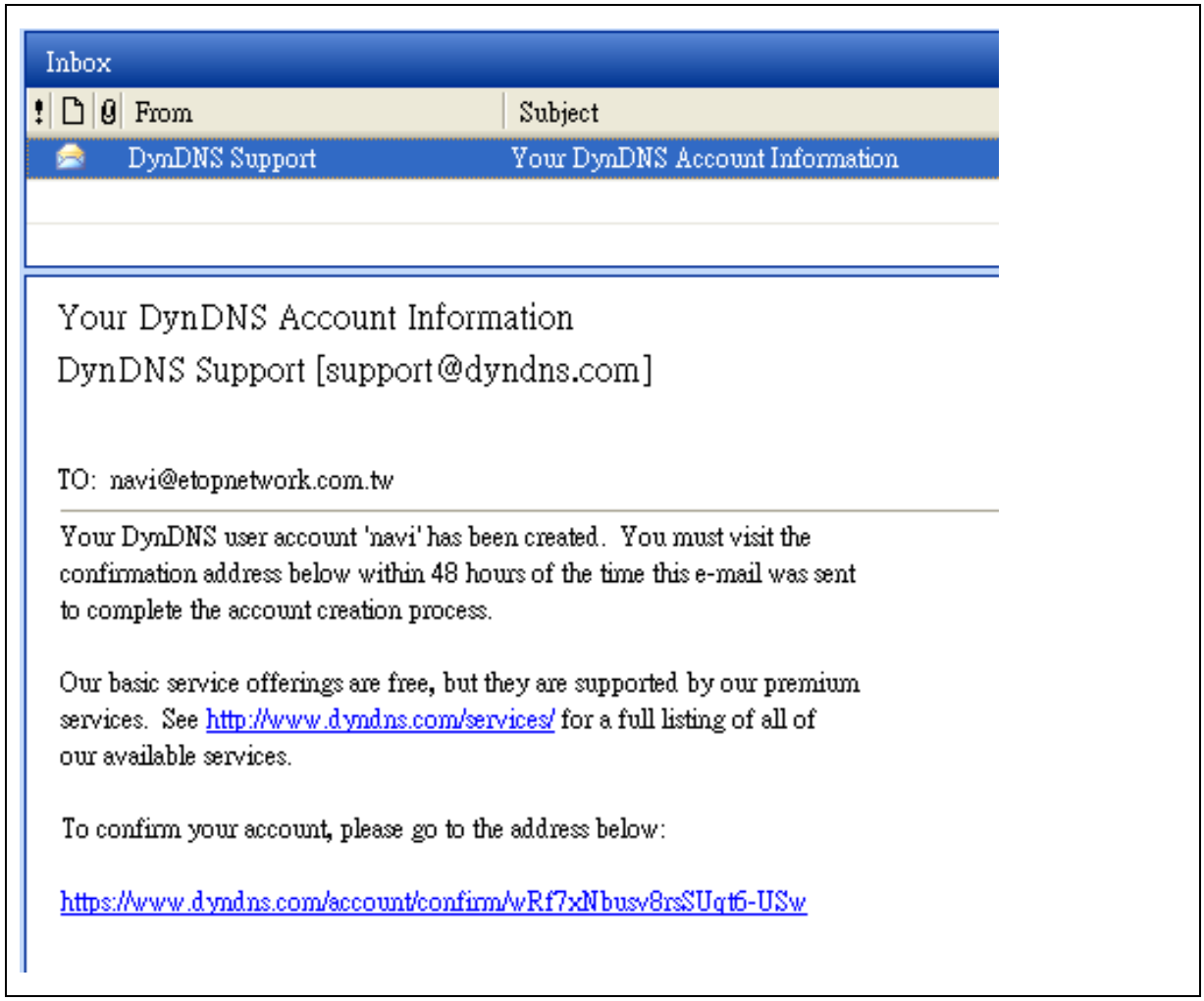
When the below window appears, you already finish the registration. Please check your E-mail box, and you will receive an e-mail from the DynDNS.


DynDNS
User:
Pass:
Login
Lost Password? - Sign Up Now
About
Services
Account
Support
News
My Account
Create Account
Login
Lost Password?
Account Created
Your account, navi , has been created. Directions for activating your account have been sent to navi @etopnetwork.com.tw. To complete registration, please follow the directions that you will receive. You must complete these steps within 48 hours to complete your registration.
You should receive the confirmation e-mail within a few minutes. Please make certain that your spam filtering allows messages from support@dyndns.com to be delivered. If you have not received this e-mail within an hour or so, request a password reset.
Following the instructions in the password reset e-mail will also confirm your new account. If you don't receive the password reset e-mail either, you should check with your e-mail provider to determine why you are not receiving these messages.

【Step 4】

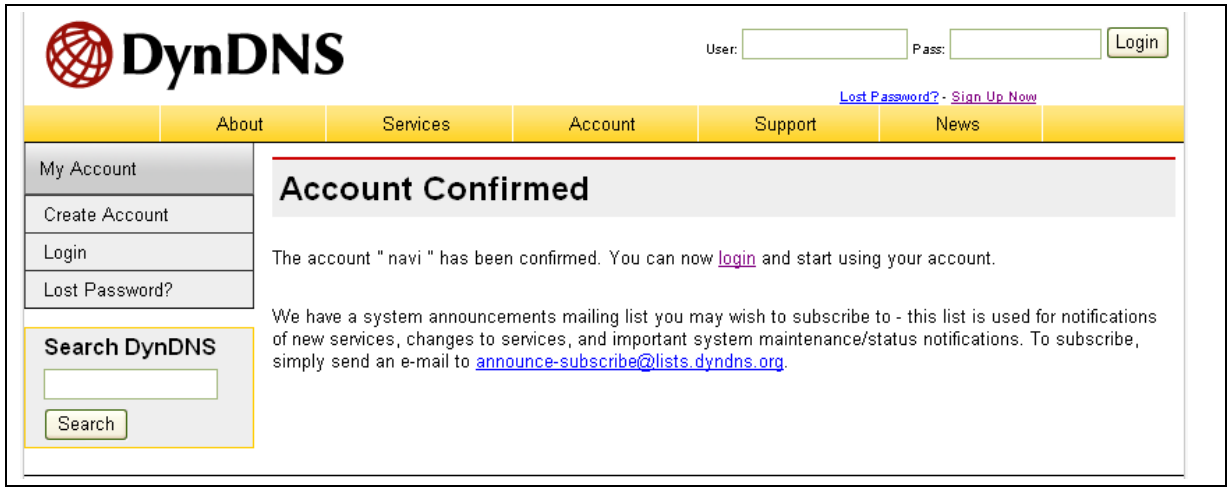
Please open the email sent from DynDNS.

Click on the link to confirm your account.


Inbox
From
Subject
DynDNS Support
Your DynDNS Account Information
Your DynDNS Account Information
DynDNS Support [support@dyndns.com]
TO: navi@etopnetwork.com.tw
Your DynDNS user account 'navi' has been created. You must visit the confirmation address below within 48 hours of the time this e-mail was sent to complete the account creation process.
Our basic service offerings are free, but they are supported by our premium services. See http://www.dyndns.com/services/ for a full listing of all of our available services.
To confirm your account, please go to the address below:
https://www.dyndns.com/account/confirm/wRf7xNbusv8rsSUqt6-USw

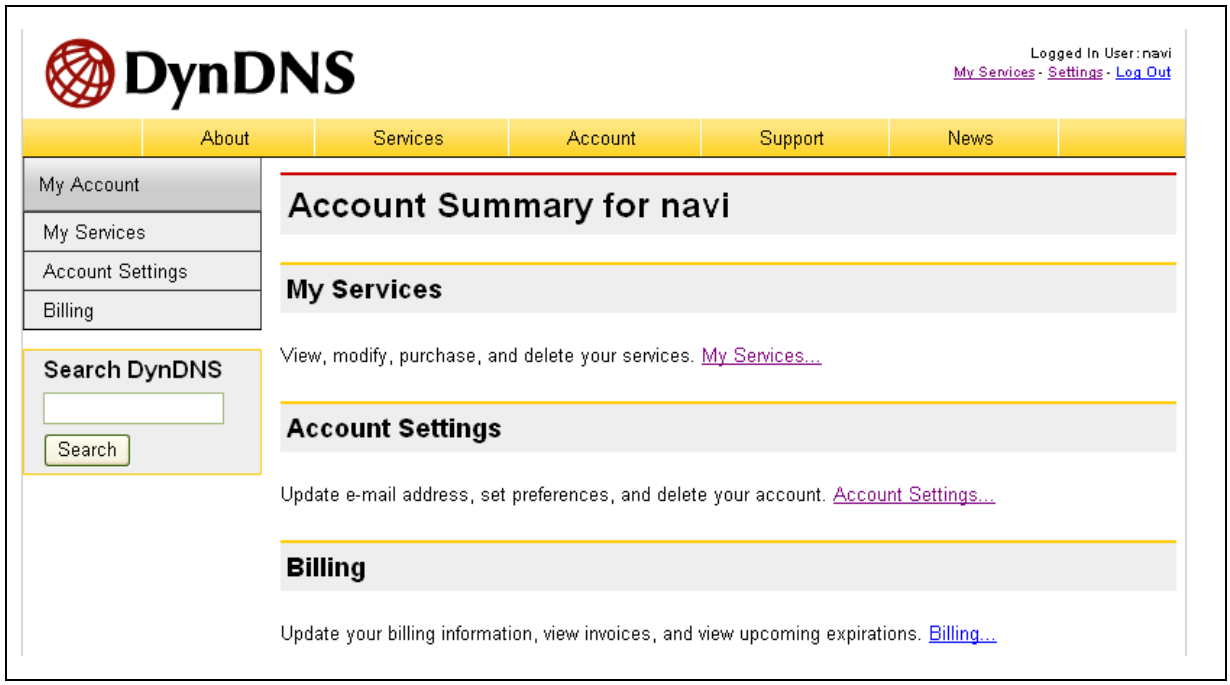
【Step 5】

Please click on **login**.


DynDNS
User:
Pass:
Login
Lost Password? - Sign Up Now
About
Services
Account
Support
News
My Account
Create Account
Login
Lost Password?
Search DynDNS
Search
Account Confirmed
The account " navi " has been confirmed. You can now login and start using your account.
We have a system announcements mailing list you may wish to subscribe to - this list is used for notifications of new services, changes to services, and important system maintenance/status notifications. To subscribe, simply send an e-mail to announce-subscribe@lists.dyndns.org.

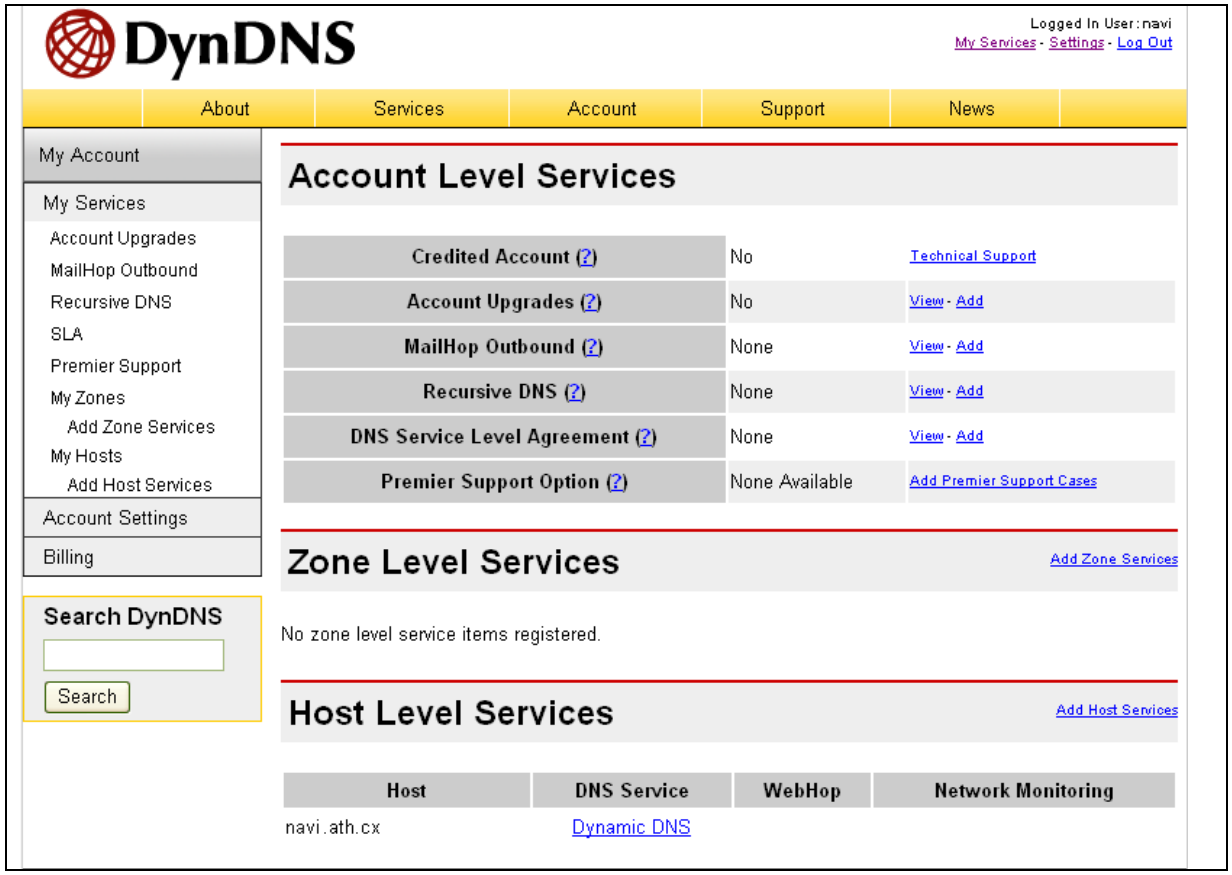
【Step 6】

Please click on **My Services** under the Account Summary for the linkage.



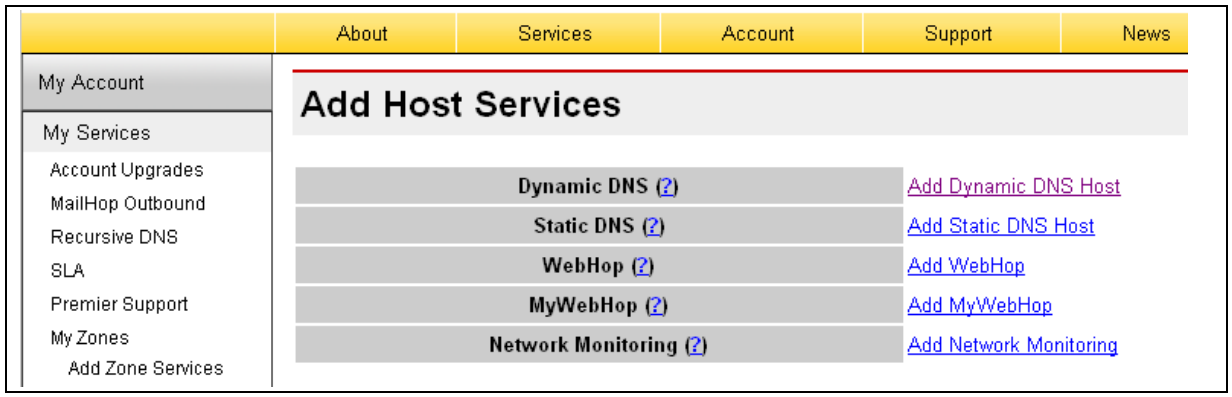
【Step 7】

Please click on **Add Host Services**.



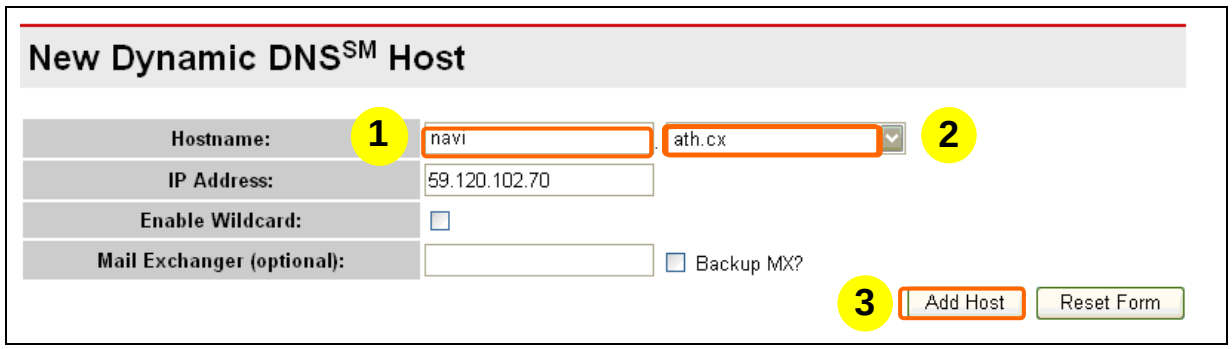
【Step 8】

Please click on **Add Dynamic DNS Host**.



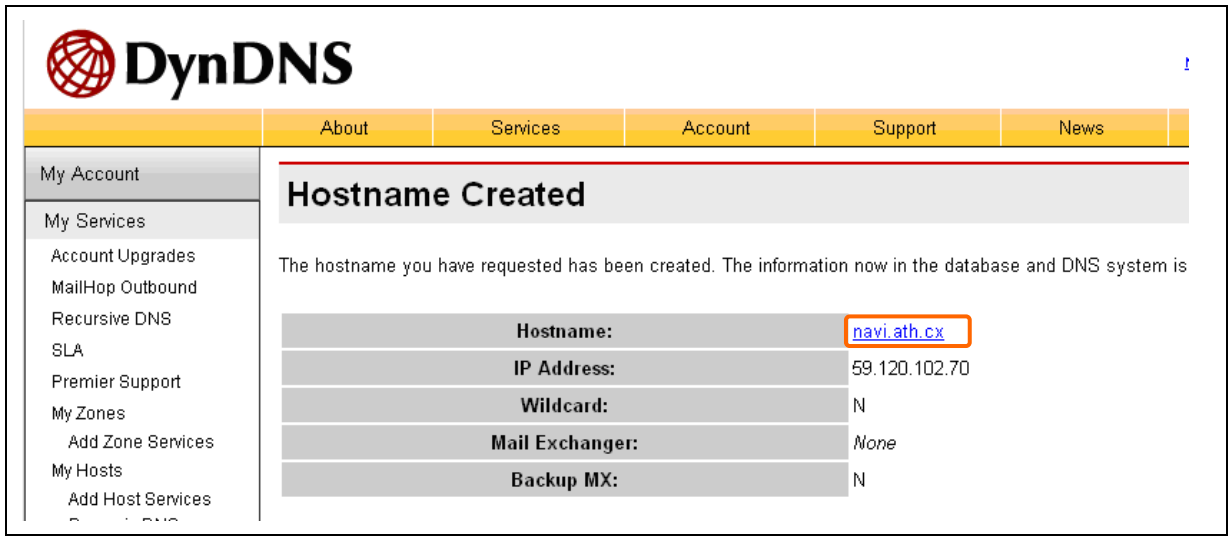
【Step 9】

1. Please input the account you applied.
2. Please select the hostname preferred at the drop-down menu.
3. Please click on **Add Host** to add the name.



【Step 10】

When the below window appears, it means your hostname is created.



Chapter 8 Q & A

8.1 Installation

1. Q: Where is the XDSL Router installed on the network?

A: In a typical environment, the Router is installed between the XDSL line and the LAN. Plug the XDSL Router into the XDSL line on the wall and Ethernet port on the Hub (switch or computer).

2. Q: Why does the throughput seem slow?

A: To achieve maximum throughput, verify that your cable doesn't exceed 100 meter. If you have to do so, we advise you to purchase a bridge to place it in the middle of the route in order to keep the quality of transmitting signal. Out of this condition you would better test something else.

- Verify network traffic does not exceed 37% of bandwidth.
- Check to see that the network does not exceed 10 broadcast messages per second.
- Verify network topology and configuration.

8.2 LED

1. Why doesn't 11n Broadband Router power up?

A: Check if the output voltage is suitable, or check if the power supply is out of order.

2. The Internet browser still cannot find or connect to 11n Broadband Router after verifying the IP address and LAN cable, the changes cannot be made, or password is lost.

A: In case 11n Broadband Router is inaccessible, you can try to restore its factory default settings. Please press the "Reset" button and keep it pressed for over 7 seconds and the light of STATUS will vanish. The LEDs will flash again when reset is successful.

3. Why does 11n Broadband Router shut down unexpectedly?

A: Re-plug your power adapter. Then, check the STATUS indicator; if it is off, the internal flash memory is damaged. For more help, please contact with your provider.

8.3 IP Address

1. Q: What is the default IP address of the router for LAN port?

A: The default IP address is 192.168.1.1 with subnet mask 255.255.255.0

2. Q: I don't know my WAN IP.

A: There are two ways to know.

Way 1: Check with your Internet Service Provider.

Way 2: Check the setting screen of 11n Broadband Router. Click on **Status & Log** item to select **Network Configuration** on the Main Menu. WAN IP is shown on the WAN interface.

3. How can I check whether I have static WAN IP Address?

A: Consult your ISP to confirm the information, or check Network Configuration in 11n Broadband Router's Main Menu.

4. Will the Router allow me to use my own public IPs and Domain, or do I have to use the IPs provided by the Router?

A: Yes, the Router mode allows for customization of your public IPs and Domain.

8.4 OS Setting

1. Why can't my computer work online after connecting to 11n Broadband Router?

A: It's possible that your Internet protocol (TCP/IP) was set to use the following IP address. Please do as the following steps. (Windows 2000 & XP) **Start**＞**Settings**＞ **Network and Dial-up Connections**＞double click on **Internet Protocol(TCP/IP)** ＞select **obtain IP address automatically**＞ Click on **OK** button. Then, open Internet browser for testing. If you still can't go online, please test something else below.

- Verify network configuration by ensuring that there are no duplicate IP addresses.
- Power down the device in question and ping the assigned IP address of the device. Ensure no other device responds to that address.

1. Check that the cables and connectors or use another LAN cable.

2. Q: Web page hangs, corrupt downloads, or nothing but junk characters is being

displayed on the screen. What do I need to do?

A: Force your NIC to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your NIC as a temporary measure. (Please look at the Network Control Panel, in your Ethernet Adapter's Advanced Properties tab.)

3. Q: Why can't I connect to the Web Configuration?

A: you can remove the proxy server settings in your web browser.

8.5 11n Broadband Router Setup

1. Q: Why does 11n Broadband Router's setup page shut down unexpectedly?

A: If one of the pages appears incompletely in 11n Broadband Router's setup pages, please click on Logout item on the Main Menu before shutting it down. Don't keep it working. Then, close Internet browser and open it again for going back to the previous page.

2. Q: Why can't my USB devices and LAN ports work properly after setting the DHCP?

A: There are two rules over here.

Rule1: After connecting USB devices, please reboot your Router.

Rule2: Before finishing the DHCP setup, please don't connect any computer to LAN ports, because the conflict of having the same IP may occur and cause some computers a lot of trouble.

※Notice: Make sure that you always click on the Apply button after configuring each setting. And in order to let other LAN ports work properly, please reboot your PC.

3. Q: I don't know how to configure DHCP.

A: DHCP is commonly used in the large local network. It allows you to manage and distribute IP addresses from 2 to 254 throughout your local network via 11n Broadband Router. Without DHCP, you would have to configure each computer separately. It's very troublesome. Please Open **Internet browser** > Input **192.168.1.1 in the website blank field** > Select **DHCP Server under** the **IP Config Menu**. For more information, please refer to 3.3.2 (Router Mode) or 4.3.1 (AP Mode).

4. Q: How do I upgrade the firmware of 11n Broadband Router?

A: Periodically, a new Flash Code is available for 11n Broadband Router on your product supplier's website. Ideally, you should update 11n Broadband Router's Flash Code using **Upgrade Firmware** on the **System Management** menu of 11n Broadband Router Settings.

5. Q: My 11N Broadband Router cannot connect to the ISP?

A: There are three possible solutions.

1. Check the Cable/XDSL modem is power on.
2. Check the Cable/XDSL link light is on to verify a good physical connection.
3. Check the WAN port LED to verify if the Cable/XDSL modem is connected to the router:

If your ISP Login method is following, please make sure the username and password are correct or not.

If your ISP is using dynamic IP addressing (DHCP) then the DHCP protocol does not have the authentication feature. Some Cable service providers often use the following to determine user's identification.

6. Q: Why is that I can ping to outside hosts, but cannot access Internet websites?

A: Check the DNS server settings on your PC. You should get the DNS servers settings from your ISP. If your PC is running a DHCP client, remove any DNS IP address setting. As the router assign the DNS settings to the DHCP-client-enabled PC.

7. Q: 11n Broadband Router couldn't save the setting after click on Apply button?

A: 11n Broadband Router will start to run after the setting finished applying, but the setting isn't written into memory. Here we suggest if you want to make sure the setting would be written into memory, please reboot the device via **Reboot** under **System Management** directory**.**

8.6 Wireless LAN

1. Q: Why couldn’t my wireless notebook work on-line after checking?

A: Generally, Wireless networks can sometimes be very complicated to set up, particularly if you're dealing with encryption and products from different vendors. Any number of variables can keep your workstations from talking to each other. Let's go over some of more common ones.

For starters, verify that your router and your workstation are using the same SSID descriptions. SSID acts as a password when a mobile device tries to connect to the wireless network. The SSID also differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A workstation will not be permitted to connect to the network unless it can provide this unique identifier. This is similar to the function of your network's Workgroup or Domain name.

When you're experiencing conductivity problems, it is always best to keep things simple. So next you are going to do is that, please disable any WEP encryption you might have configured.

Successful implementation of encryption also includes the use of a shared key. A HEX key is the most common, but other formats are also used. This key identifies the workstation to the router as a trusted member of this network. Different manufacturers can implement this key technology in ways that might prevent them from working correctly with another vendor's products. So pay attention to detail is going to be the key to a successful installation.

Next make sure the router and the NIC are configured to use the same communications channel. There are normally 11 of them, and the default channel can also vary from vendor to vendor. You might also want to confirm that the router has DHCP services enabled and an address pool configured. If not, the NIC won't be able to pick up an IP address. I have run across a few access points that offer DHCP services but do not assign all of the needed IP information to the NIC. As a result, I was able to connect to the network, but could not browse the web. The point is, don't assume anything. Verify for yourself that all of the required settings are being received by the workstation.

Finally, you might want to keep the system you're trying to configure in the same room as the router, at least during the initial configuration, in order to minimize potential interference from concrete walls or steel beams.

2. Q: My PC can't locate the Wireless Access Point.

A: Check the following:

- Your PC is set to Infrastructure Mode. (Access Points are always in Infrastructure Mode.)
- The SSID on your PC and the Wireless Access Point are the same. Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup".
- Both your PC and the Wireless Access Point must have the same setting for WEP. The default setting for the Wireless Router is disabled, so your wireless station should also have WEP disabled.
- If WEP is enabled on the Wireless Router, your PC must have WEP enabled, and the key must match.
- If the Wireless Router's Wireless screen is set to Allow LAN access to selected Wireless Stations only, then each of your Wireless stations must have been selected, or access will be blocked.
- To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Access Point. Remember that the connection range can be as little as 100 feet in poor environments.

3. Q: Wireless connection speed is very slow.

A: The wireless system will connect at highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with following:

- Access Point location: Try adjusting the location and orientation of the Access Point.
- Wireless Channel: If interference is the problem, changing to another channel may show a marked improvement.
- Radio Interference: Other devices may be causing interference. You can experiment by switching other devices off, and see if this helps. Any "noisy" devices should be shielded or relocated.
- RF Shielding: Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Access Point.

4. Q: Some applications do not run properly when using the Wireless Router.

A: The Wireless Router processes the data passing through it, so it is not transparent. Use the Special Application feature to allow the use of Internet applications which do not function correctly. If this does solve the problem, you can use the DMZ function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.

5. Q: I can't connect to the Wireless Router to configure it.

A: Check the following:

- The Wireless Router is properly installed, LAN connections are OK, and it is powered ON.
- Make sure that your PC and the Wireless Router are on the same network segment.
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, make sure that it is using an IP Address within the range 192.168.1.129 to 192.168.1.253 and thus compatible with the Wireless Router's default IP Address of 192.168.1.254. Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Router. In Windows, you can check these settings by using Control Panel ~ Network to check the Properties for the TCP/IP protocol.

6. Q: The WinXP wireless interface couldn't communicate the WEP with 11n Broadband Router's wireless interface.

A: The default WEP of WinXP is **Authentication Open System - WEP**, but the WEP of 11n Broadband Router is only for **Shared Key - WEP**, it caused both sides couldn't communicate. Please select the WEP of WinXP from Authentication Open System to **Pre-shared Key - WEP**, and then the WEP wireless interface between WinXP and 11n Broadband Router would be communicated.

8.7 Support

1. Q: What is the maximum number of IP addresses that the XDSL Router will support?

A: The Router will support to 253 IP addresses with NAT mode.

5. Q: Is the Router cross-platform compatible?

A: Any platform that supports Ethernet and TCP/IP is compatible with the Router.

8.8 Others

1. Q: Why can't I receive corrupted FTP downloads?

A: If you are experiencing corrupted files when you download a file with your FTP client, try using another FTP program.

2. Q: Why does the router dial out for PPPoE mode very often?

A: Normally some of game, music or anti-virus program will send out packets that trigger the router to dial out, you can close these programs. Or you can set the idle time to 0, then control to dial out manually.

3. Q: What can I do if there is already a DHCP server in LAN?

A: If there are two DHCP servers existing on the same network, it may cause conflict and generate trouble. In this situation, we suggest to disable DHCP server in router and configure your PC manually.